VMware Horizon Client for iOS Installation and Setup Guide

VMware Horizon Client for iOS 2006

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

VMware Horizon Client for iOS Installation and Setup Guide

This guide provides information about installing, configuring, and using VMware Horizon® Client™ software on an iOS device.

This information is intended for administrators who need to set up a VMware Horizon deployment that includes iOS client devices. The information is written for experienced system administrators who are familiar with virtual machine technology and data center operations.

If you are an end user, see the *VMware Horizon Client for iOS User Guide* document, or view the Horizon Client online help.

Setup and Installation

1

Setting up a VMware Horizon deployment for iOS clients involves using certain Connection Server configuration settings, meeting the system requirements for VMware Horizon servers and iOS clients, and installing the app for Horizon Client.

This chapter includes the following topics:

System Requirements

iOS devices that run Horizon Client must meet certain hardware and software requirements.

System Requirements for iOS Clients

The iOS device on which you install Horizon Client, and the peripherals it uses, must meet certain system requirements.

Operating systems

- iOS 11.x

- iOS 12.x
- iOS 13.x
- iPadOS 13.x

(Optional) External keyboards

iPad Keyboard Dock and Apple Wireless Keyboard (Bluetooth).

Smart card authentication

See Smart Card Authentication Requirements.

Touch ID authentication

See Touch ID Authentication Requirements.

Face ID authentication

See Face ID Authentication Requirements.

Connection Server and Horizon Agent

Latest maintenance release of Horizon 7 version 7.5 and later releases.

If client devices connect from outside the corporate firewall, use a Unified Access Gateway appliance so that client devices do not require a VPN connection. If your company has an internal wireless network to provide routable access to remote desktops that devices can use, you do not need to set up Unified Access Gateway or a VPN connection.

Display protocols

- PCoIP
- VMware Blast

Network protocols

- IPv4
- IPv6

For information about using Horizon in an IPv6 environment, see the *Horizon Installation* document.

System Requirements for Real-Time Audio-Video

Real-Time Audio-Video works with standard audio and video devices and with standard conferencing applications such as Skype, WebEx, and Google Hangouts. To support Real-Time Audio-Video, your Horizon environment must meet certain software and hardware requirements.

Remote desktops and published applications

Horizon Agent 7.5 or later.

Client access device

Real-Time Audio-Video is supported on all iOS devices that run Horizon Client for iOS. For more information, see System Requirements for iOS Clients .

Smart Card Authentication Requirements

Client devices that use a smart card for user authentication must meet certain requirements.

Using the Derived Credentials Feature

To use the derived credentials feature, a Horizon administrator must install smart card middleware on the virtual desktops or RDS host that hosts published desktops. No other middleware for PIV cards must be installed on the same virtual desktops or RDS host. VMware has tested Charismathics CSSI/CSTC 5.2.2 and ActivClient 7.1. The Windows Inbox Smart Card Minidriver is not supported.

On the client device, you must use the Purebred app to create a derived credential and provision the credential to the client device, create a virtual smart card, and pair the virtual smart card with the smart card middleware installed on the remote desktop. For information, see Create a Virtual Smart Card and Pair a Virtual Smart Card with Smart Card Middleware.

Enabling the User Name Hint Text Box in Horizon Client

In some environments, smart card users can use a single smart card certificate to authenticate to multiple user accounts. Users enter their user name in the **Username hint** text box when they sign in with a smart card.

To make the **Username hint** text box appear on the Horizon Client login dialog box, you must enable the smart card user name hints feature in Connection Server. For information about enabling the smart card user name hints feature, see the *Horizon Administration* document.

If your environment uses a Unified Access Gateway appliance for secure external access, you must configure the Unified Access Gateway appliance to support the smart card user name hints feature. The smart card user name hints feature is supported only with Unified Access Gateway 2.7.2 and later. For information about enabling the smart card user name hints feature in Unified Access Gateway, see the *Deploying and Configuring VMware Unified Access Gateway* document.

Horizon Client continues to support single-account smart card certificates even when the smart card user name hints feature is enabled.

Additional Smart Card Authentication Requirements

In addition to meeting the smart card requirements for Horizon Client systems, other Horizon components must meet certain configuration requirements to support smart cards.

Connection Server and security server hosts

An administrator must add all applicable Certificate Authority (CA) certificate chains for all trusted user certificates to a server truststore file on the Connection Server host or, if a security server is used, on the security server host. These certificate chains include root certificates and, if an intermediate certificate authority issues the user's smart card certificate, must also include intermediate certificates.

For information about configuring Connection Server to support smart card use, see the *Horizon Administration* document.

Unified Access Gateway appliances

For information about configuring smart card authentication on a Unified Access Gateway appliance, see the *Deploying and Configuring VMware Unified Access Gateway* document.

Active Directory

For information about tasks that an administrator might need to perform in Active Directory to implement smart card authentication, see the *Horizon Administration* document.

Touch ID Authentication Requirements

To use Touch ID for user authentication in Horizon Client, you must meet certain requirements.

iPad and iPhone models

Any iPad or iPhone model that supports Touch ID, for example, iPad Air 2 and iPhone 6.

Operating system requirements

- iOS 8 or later.
- Add at least one fingerprint in the Touch ID & Passcode setting.

Connection Server requirements

- Horizon 7 version 7.5 or later.
- Enable biometric authentication in Connection Server. For information, see "Configure Biometric Authentication" in the *Horizon Administration* document.
- The Connection Server instance must present a valid root-signed certificate to Horizon Client.

Horizon Client requirements

- Set the certificate checking mode to **Never connect to untrusted servers** or **Warn before connecting to untrusted servers**. For information about setting the certificate checking mode, see Setting the Certificate Checking Mode in Horizon Client.
- Enable Touch ID by tapping the Touch ID (fingerprint) icon in the **Password** text box on the server login window. After you successfully log in, your Active Directory credentials are stored securely in the iOS device's Keychain.

You can use Touch ID with smart card authentication and as part of two-factor authentication with RSA SecurID and RADIUS authentication. If you use Touch ID with smart card authentication, Horizon Client connects to the server after you enter your PIN and the Touch ID login window does not appear.

Face ID Authentication Requirements

To use Face ID for user authentication in Horizon Client, you must meet certain requirements.

iPad and iPhone models

Any iPad or iPhone model that supports Face ID, such as iPhone X.

Operating system requirements

- iOS 11 or later.
- Add a Face ID scan in the Face ID & Passcode setting.

Connection Server requirements

- Horizon 7 version 7.5 or later.
- Enable biometric authentication in Connection Server. For information, see "Configure Biometric Authentication" in the *Horizon Administration* document.
- The Connection Server instance must present a valid root-signed certificate to Horizon Client.

Horizon Client requirements

- Set the certificate checking mode to **Never connect to untrusted servers** or **Warn before connecting to untrusted servers**. For information about setting the certificate checking mode, see Setting the Certificate Checking Mode in Horizon Client.
- Enable Face ID by tapping the Face ID (face) icon in the **Password** text box on the server login window. After you successfully log in, your Active Directory credentials are stored securely in the iOS device's Keychain.

You can use Face ID with smart card authentication and as part of two-factor authentication with RSA SecurID and RADIUS authentication. If you use Face ID with smart card authentication, Horizon Client connects to the server after you enter your PIN and the Face ID login window does not appear.

OPSWAT Integration Requirements

At some companies, an administrator might integrate Unified Access Gateway with the third-party OPSWAT MetaAccess application. This integration, which is typically used on unmanaged devices in corporate bring-your-own-device (BYOD) environments, enables organizations to define device acceptance policies for Horizon Client devices.

For example, an administrator might define a device acceptance policy that requires client devices to be password protected or have a minimum operating system version. Client devices that comply with the device acceptance policy can access remote desktops and published applications through Unified Access Gateway. Unified Access Gateway denies access to remote resources from client devices that do not comply with the device acceptance policy.

To use OPSWAT integration, the following requirements must be met.

- An administrator must configure the Endpoint Compliance Checks feature in Unified Access Gateway. Unified Access Gateway 3.8 or later is required. For information, see the *Deploying and Configuring VMware Unified Access Gateway* document.
- You must install OPSWAT Mobile App on the client device. You can download OPSWAT Mobile App from the App Store.

Horizon Client generates a device ID that is unique to the client device. When you start Horizon Client, and OPSWAT Mobile App is installed, Horizon Client prompts you to share the device ID with OPWSAT Mobile App. To share the device ID, tap **Share**. If you tap **Never ask again**, Horizon Client does not share the device ID and you are not prompted again. To close the dialog box, tap **Cancel**.

If you tap **Share**, OPSWAT verifies the client device's security status and sends a compliance report to the MetaAccess server. If the client device is already registered with OPSWAT, it is enrolled successfully. If the device is not registered with OPSWAT, an error message appears and the device is not enrolled. To return to Horizon Client, tap **Return**.

You can configure device ID sharing by enabling or disabling a setting in Horizon Client. For more information, see Configure Device ID Sharing with OPSWAT.

Supported Desktop Operating Systems

A Horizon administrator creates virtual machines that have a guest operating system and installs agent software in the guest operating system. End users can log in to these virtual machines from a client device.

For a list of the supported Windows guest operating systems, see the *Horizon Installation* document.

Some Linux guest operating systems are also supported. For information about system requirements, configuring Linux virtual machines, and a list of supported features, see the *Setting Up Linux Desktops in Horizon* document.

Preparing Connection Server for Horizon Client

Before end users can connect to a server and access a remote desktop or published application, a Horizon administrator must configure certain Connection Server settings.

Unified Access Gateway and Security Servers

If your VMware Horizon deployment includes a Unified Access Gateway appliance, configure Connection Server to work with Unified Access Gateway. See the *Deploying and Configuring VMware Unified Access Gateway* document. Unified Access Gateway appliances perform the same role as security servers.

If your VMware Horizon deployment includes a security server, verify that you are using the latest maintenance releases of Connection Server 7.5 and Security Server 7.5 or later releases. For more information, see the installation document for your Horizon version.

Note Security servers are not supported in VMware Horizon 2006 and later.

Secure Tunnel Connection

If you plan to use a secure tunnel connection for client devices, and if the secure connection is configured with a DNS host name for a Connection Server instance or a security server, verify that the client device can resolve this DNS name. .

Desktop and Application Pools

Use the following check list when configuring desktop and application pools.

- Verify that a desktop or application pool has been created and that the user account that you plan to use is entitled to access the pool. For more information, see the *Setting Up Virtual Desktops in Horizon* and *Setting Up Published Desktops and Applications in Horizon* documents.
- Verify that the desktop or application pool is set to use the VMware Blast display protocol or the PCoIP display protocol. For information, see the *Setting Up Virtual Desktops in Horizon* and *Setting Up Published Desktops and Applications in Horizon* documents.

User Authentication

Use the following check list when setting up user authentication.

- To use Touch ID or Face ID authentication with Horizon Client, you must enable biometric authentication in Connection Server. For more information, see the *Horizon Administration* document.
- To enable end users to save their passwords with Horizon Client, so that they do not have to supply credentials when they connect to a Connection Server instance, configure Horizon LDAP for this feature in Connection Server.

  Users can save their passwords if Horizon LDAP is configured to allow it, if the Horizon Client certificate verification mode is set to **Warn before connecting to untrusted servers** or **Never connect to untrusted servers**, and if Horizon Client can fully verify the server certificate that Connection Server presents. For more information, see the *Horizon Administration* document.

- To use two-factor authentication, such as RSA SecurID or RADIUS authentication, with Horizon Client, you must enable the two-factor authentication feature for the Connection Server instance. Beginning with Horizon 7 version 7.11, you can customize the labels on the RADIUS authentication login page. Beginning with Horizon 7 version 7.12, you can configure two-factor authentication to occur after a remote session times out. For more information, see the topics about two-factor authentication in the *Horizon Administration* document.
- To hide the server URL in Horizon Client, enable the **Hide server information in client user interface** global setting. For more information, see the *Horizon Administration* document.
- To hide the **Domain** drop-down menu in Horizon Client, enable the **Hide domain list in client user interface** global setting. Beginning with Horizon 7 version 7.8, this setting is enabled by default. For more information, see the *Horizon Administration* document.
- To send the domain list to Horizon Client, enable the **Send domain list** global setting in Horizon Console. This setting is available in Horizon 7 version 7.8 and later and is disabled by default. Earlier Horizon 7 versions send the domain list. For more information, see the *Horizon Administration* document.

The following table shows how the **Send domain list** and **Hide domain list in client user interface** global settings determine how users can log in to the server.

Send domain list setting	Hide domain list in client user interface setting	How users log in
Disabled (default)	Enabled	The **Domain** drop-down menu is hidden. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ *domain\username* ■ *username@domain.com*
Disabled (default)	Disabled	If a default domain is configured on the client, the default domain appears in the **Domain** drop-down menu. If the client does not know a default domain, `*DefaultDomain*` appears in the **Domain** drop-down menu. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ *domain\username* ■ *username@domain.com*
Enabled	Enabled	The **Domain** drop-down menu is hidden. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ *domain\username* ■ *username@domain.com*
Enabled	Disabled	Users can enter a user name in the **User name** text box and then select a domain from the **Domain** drop-down menu. Alternatively, users can enter one of the following values in the **User name** text box. ■ *domain\username* ■ *username@domain.com*

Installing Horizon Client

You can install Horizon Client the same way that you install other iOS apps. You can also configure VMware Workspace ONE UEM to deliver Horizon Client to end users.

Install or Upgrade Horizon Client on an iOS Device

You can install Horizon Client from the VMware Downloads page or from the App Store.

Prerequisites

- If you have not already set up the iOS device, do so. For information, see the user guide from Apple.
- Verify that you have the URL for a download page that contains the Horizon Client installer. This URL might be the VMware Downloads page at http://www.vmware.com/go/viewclients, or it might be the URL for a Connection Server instance.

Procedure

1. On the iOS device, Mac, or PC, browse to the URL for downloading the installer file, or search the App Store for the Horizon Client app.
2. Download the app.
3. If you downloaded the app to a Mac or PC, connect the iOS device to the computer and follow the onscreen instructions in iTunes.
4. To determine whether the installation succeeded, verify that the **Horizon** app icon appears on the iOS device.

Configure Workspace ONE UEM to Deliver Horizon Client to iOS Devices

You can configure Workspace ONE UEM to deliver Horizon Client to iOS device users.

You can optionally specify a default list of Connection Server instances. The Connection Server instances that you specify appear as shortcuts in Horizon Client.

Prerequisites

- Install and deploy Workspace ONE UEM. See https://my.workspaceone.com/products/Workspace-ONE-UEM.
- Become familiar with the Workspace ONE UEM console. For more information, see the Workspace ONE UEM product documentation at https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/index.html.

Procedure

1. Log in to the Workspace ONE UEM console as an administrator.

2 Select **Accounts > Users > List View**, click **Add User**, and add user accounts for the users who will run Horizon Client on their mobile devices.

3 Select **Accounts > Users > User Groups**, click **Add**, and create a user group for the user accounts that you created.

4 Upload and add the Horizon Client application.

   a Select **Apps & Books > Applications > List View** and click **Add Application** on the **Public** tab.

   b Search for and select VMware Horizon Client for Apple iOS in the App Store.

   c On the **Info** tab, type an application name and specify the supported iOS device models.

   d On the **Assignment** tab, assign the Horizon Client application to the user group that you created.

e (Optional) Configure one or more default servers.

You can configure only one of the following options. Configuring both options at the same time is not supported.

Note This feature is supported only for iOS 7 and later devices. You cannot push a default Connection Server list to an iOS 6 device.

Option	Description
Configure server, user name, and domain information	On the **Deployment** tab, select a push mode, select the **Send Application Configuration** check box, enter **broker_list** in the **Configuration Key** text box, select **String** from the **Value Type** drop-down menu, and enter a list of default servers in the **Configuration Value** text box in JSON format. Use the **server** property to specify the IP address or host name of the server, the **username** and **domain** properties to specify the name and domain of a user that is entitled to the server, and the **description** property to specify a description of the server. The following example specifies four default servers. `{"settings":{ "server_list":[{"server":"123.456.1.1","description":"View server 1"}, {"server":"123.456.1.2","description":"View server 2"}, {"server":"123.456.1.3","description":"View server 3"}, {"server":"viewserver4.mydomain.com","description":"View server 4","username":"vmware","domain":"view"}]}}`
Configure server information only	On the **Deployment** tab, select a push mode, select the **Send Application Configuration** check box, enter **servers** in the **Configuration Key** text box, select **String** from the **Value Type** drop-down menu, and enter the IP address or host name of a server in the **Configuration Value** text box. **servers** is case sensitive. To specify a list of servers, enter multiple IP addresses or host names, separated by commas, in the **Configuration Value** text box. The following example specifies three default servers. `123.456.1.1, viewserver4.mydomain.com, 123.456.1.2`

The servers that you specify appear as shortcuts in VMware Horizon Client.

f (Optional) To configure camera settings, enter **settings** in the **Configuration Key** text box, select **String** from the **Value Type** drop-down menu, and enter the camera settings in the **Configuration Value** text box in JSON format.

Use the **camera_position** property to specify the camera position and the **video_quality** property to specify the video quality. Valid **camera_position** properties are **front** and **rear**. Valid **video_quality** properties are **default**, **high**, **medium**, and **low**.

For example:

```
{"camera": {
"camera_position":"rear",
"video_quality":"medium"
}}
```

g Publish the Horizon Client application.

5 Install and set up the Workspace ONE UEM Agent on each iOS device.

You can download the Workspace ONE UEM Agent from iTunes.

6 Use the Workspace ONE UEM console to install the Horizon Client application on the mobile devices.

You cannot install the Horizon Client application before the effective date on the **Deployment** tab.

Results

Workspace ONE UEM delivers Horizon Client to the iOS devices in the user group that you associated with the Horizon Client application.

When a user launches Horizon Client, Horizon Client communicates with the Workspace ONE UEM Agent on the device. If you configured a default list of Connection Server instances, Workspace ONE UEM pushes the server information to the Workspace ONE UEM Agent on the device and shortcuts for those servers appear in Horizon Client.

Later, you can use the Workspace ONE UEM console to modify, delete, or add Connection Server instances to the server list and push those changes to iOS devices. When pushing a new server list from Workspace ONE UEM to iOS devices, Horizon Client uses the following rules.

- If the new server list contains a server that does not exist in the device's server list, Horizon Client adds the server to the beginning of the device's server list.
- If the new server list contains a server that is already in the device's server list, it's position in the device's server list is unchanged.
- If the new server list does not contain a server that is in the device's server list, Horizon Client deletes the server from the device's server list.

Using Embedded RSA SecurID Software Tokens

If you create and distribute RSA SecurID software tokens to end users, users need enter only their PIN, rather than their PIN and a token code, to authenticate.

Setup Requirements

You can use Compressed Token Format (CTF) or dynamic seed provisioning, which is also called CT-KIP (Cryptographic Token Key Initialization Protocol), to set up an easy-to-use RSA authentication system. With this system, you generate a URL to send to end users. To install the token, end users paste this URL directly into Horizon Client on their client devices. The dialog box for pasting this URL appears when end users connect to a Connection Server instance with Horizon Client.

After the software token is installed, end users enter a PIN to authenticate. With external RSA tokens, end users must enter a PIN and the token code generated by a hardware or software authentication token.

The following URL prefixes are supported for end users that copy and paste the URL into Horizon Client when Horizon Client is connected to an RSA-enabled Connection Server instance:

- `viewclient-securid://`
- `com.rsa.securid.iphone://`
- `com.rsa.securid://`

For end users that install the token by tapping the URL, only the `viewclient-securid://` prefix is supported.

For information about using dynamic seed provisioning or file-based (CTF) provisioning, see the Web page *RSA SecurID Software Token for iPhone Devices* at http://www.rsa.com/node.aspx?id=3652 or *RSA SecurID Software Token for Android* at http://www.rsa.com/node.aspx?id=3832.

Instructions to End Users

When you create a CTFString URL or CT-KIP URL to send to end users, you can generate a URL with or without a password or activation code. Send this URL to end users in an email that includes the following information.

- Instructions for navigating to the Install Software Token dialog box.

  Instruct end users to tap **External Token** in the Horizon Client dialog box that prompts them for RSA SecurID credentials when they connect to a Connection Server instance.

- CTFString URL or CT-KIP URL in plain text.

  If the URL has formatting on it, end users receive an error message when they try to use it in Horizon Client.

- Activation code, if the CT-KIP URL that you create does not already include the activation code.

End users must enter this activation code in a text box of the dialog box.

- If the CT-KIP URL includes an activation code, instruct end users that they need not enter a value in the **Password or Activation Code** text box in the Install Software Token dialog box.

Create a Virtual Smart Card

To use the derived credentials feature, you must create a virtual smart card to use when you log in to a server and connect to a remote desktop. One virtual smart card can hold multiple certificates.

Prerequisites

- Verify that the client device, remote desktops, RDS hosts, Connection Server host, and other Horizon components meet the smart card authentication requirements. See Smart Card Authentication Requirements.
- Use the Purebred app to create a derived credential and provision the credential on the client device.
- Verify that the device has a passcode. A passcode is required to create a virtual smart card.

Procedure

1. Tap **Settings** at the bottom of the Horizon Client window.
2. Tap **Derived Credentials** and then tap **Create New Virtual Smartcard**.
3. Perform device authentication.
   - If either Touch ID or Face ID is enabled, authenticate with Touch ID or Face ID.
   - If neither Touch ID nor Face ID is enabled, authenticate with a passcode.
4. Enter and confirm a PIN for the virtual smart card.
5. Tap **Continue** and import the derived credential from the Purebred key chain.
   a. Tap **PIV Authentication Certificate**.
   b. Select the **Purebred Key Chain** location.
   c. Select the certificate to import.
6. (Optional) To import a digital signature certificate or encryption certificate after you import the PIV authentication certificate, tap **Digital Signature Certificate** or **Encryption Certificate** and follow the prompts.
7. To create the virtual smart card, tap **Done**.

   The derived credential appears in the **Settings** window. The **Use Derived Credentials** setting is set to on.
8. To create another virtual smart card for a different Horizon environment, tap **Create new virtual smartcard** and repeat these steps.

What to do next

Pair a Virtual Smart Card with Smart Card Middleware.

Manage a Virtual Smart Card

You can reset the PIN for a virtual smart card in Horizon Client. You can also delete a virtual smart card. After you log in to a remote desktop with a virtual smart card, you can also use the Charismathics Security Token Configurator in the remote desktop to view the certificate and key, manage, and change the user PIN for the virtual smart card.

Prerequisites

Create a Virtual Smart Card.

Procedure

- To reset the PIN for a virtual smart card, perform these steps.
  a. Tap **Settings** at the bottom of the Horizon Client window.
  b. Tap **Derived Credentials**.
  c. Tap the virtual smart card.
  d. Tap **Reset PIN**.
  e. Enter the current PIN, enter and confirm the new PIN, and tap **Done**.
- To remove a virtual smart card, perform these steps.
  a. Tap **Settings** at the bottom of the Horizon Client window.
  b. Tap **Derived Credentials**.
  c. Touch the virtual smart card, slide your finger to the left, and tap **Delete**.

Pair a Virtual Smart Card with Smart Card Middleware

To use the derived credentials feature, you must create a group policy object (GPO) in Active Directory that pairs a virtual smart card with the smart card middleware installed on the remote desktop. You then apply the GPO to the organizational unit (OU) that contains the remote desktop.

Prerequisites

- Verify that the system requirements for using derived credentials are met. See Smart Card Authentication Requirements.
- Create a Virtual Smart Card.
- Verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server.

- Verify that the MMC and Group Policy Management Editor snap-in are available on your Active Directory server.

Procedure

1. On the Active Directory server, open the Group Policy Management Console (`gpmc.msc`).
2. Right-click **Group Policy Objects** and select **New**.
3. In the **Name** text box, type a name for the group policy object, for example, `Derived Credentials`, and click **OK**.
4. Right-click the group policy object that you created and select **Edit**.
5. Expand **Computer Configuration > Preferences > Windows Settings** .
6. Right-click **Registry** and select **New > Collection Item**.
7. Change the collection item name from `Collection` to a meaningful name, for example, the middleware name `Charismathics`.
8. To create registry items that pair a virtual smart card with the smart card middleware installed in the remote desktop, right-click the collection item that you created and select **New > Registry Item**.

   To pair a virtual smart card with Charismathics middleware, use the following values.

   - `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\VMware Remote Smart Card]`
   - `"ATR"=hex:3b,1c,96,56,4d,57,61,72,65,43,61,72,64,23,31`
   - `"Crypto Provider"="Charismathics Smart Security Interface CSP"`

   To pair a virtual smart card with ActivClient middleware, use the following values.

   - `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\VMware Remote Smart Card]`
   - `"80000001"="C:\\Program Files\\HID Global\\ActivClient\\ac.scapi.scmd.dll"`
   - `"ATR"=hex:3b,1c,96,56,4d,57,61,72,65,43,61,72,64,23,31`
   - `"ATRMask"=hex:ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff`
   - `"Crypto Provider"="Microsoft Base Smart Card Crypto Provider"`
   - `"Smart Card Key Storage Provider"="Microsoft Smart Card Key Storage Provider"`
9. Open the Group Policy Management Editor and link the new GPO to the OU that contains the remote desktop.

   For a virtual desktop, link the GPO to the OU that contains the virtual desktop. For a published desktop, link the GPO to the OU that contains the RDS host.
10. To verify the registry settings in the remote desktop, restart the remote desktop or open the remote desktop and run `cmd gpudate /force`.

What to do next

Log in to the server and connect to the remote desktop. The process is the same as when you use a physical smart card.

Note If you enter the wrong PIN more than five times when using a virtual smart card to authenticate, the virtual smart card is removed and you must create a new virtual smart card.

Configure Device ID Sharing with OPSWAT

If OPSWAT Mobile App is installed on the client device, you are prompted to share the client device ID when you start Horizon Client. You can also enable or disable device ID sharing by configuring a setting in Horizon Client.

Prerequisites

Configure OPSWAT integration. See OPSWAT Integration Requirements.

Procedure

1. Tap **Settings** at the bottom of the Horizon Client window and tap **Share Device ID with OPSWAT**.
2. Tap to toggle the **Share Device ID with OPSWAT** option to on or off.

   If you toggle the setting to off, the setting is disabled and Horizon Client prompts you to share the device ID the next time you start Horizon Client.

   If you toggle the setting to on, you must select one of the following options.

Option	Description
Share	Horizon Client shares the device ID with OPSWAT. OPSWAT verifies the client device's security status and sends a compliance report to the MetaAccess server. If the client device is already registered with OPSWAT, it is enrolled successfully. If the device is not registered with OPSWAT, an error message appears and the device is not enrolled. To return to Horizon Client, tap **Return**.
Never ask again	Horizon Client does not share the device ID with OPSWAT and it does not prompt you to share the device ID again.
Cancel	Horizon Client prompts you to share the device ID the next time you start Horizon Client.

Configure Advanced TLS Options

You can select the security protocols and cryptographic algorithms that Horizon uses to encrypt communications between Horizon Client and servers, and between Horizon Client and Horizon Agent.

By default, TLS v1.1 and TLS v1.2 are enabled. SSL v2.0, SSL v3.0, and TLS v1.0 are not supported. The default cipher control string is "!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA +AESGCM:kECDH+AES:ECDH+AES:RSA+AES".

If you configure a security protocol for Horizon Client that is not enabled on the server to which the client system connects, a TLS error occurs and the connection fails.

For information about configuring the security protocols that Connection Server can accept, see the *Horizon Security* document.

Procedure

1. Tap **Settings** at the bottom of the Horizon Client window.
2. Tap **Advanced SSL Options**.
3. Verify that the **Reset to Default Settings** option is set to off.
4. To enable or disable a security protocol, tap the **On** or **Off** toggle next to the security protocol name.
5. To change the cipher control string, replace the default string.
6. (Optional) To revert to the default settings, tap **Reset** in the upper right corner of the window.

Results

Your changes take effect the next time you connect to the server.

Configure VMware Blast Options

You can configure VMware Blast options for remote desktop and published application sessions that use the VMware Blast display protocol.

You can configure H.264 decoding before or after you connect to a server. H.264 is an industry standard for video compression, which is the process of converting digital video into a format that takes up less capacity when it is stored or transmitted.

After you connect to a server, the **VMware Blast** setting is visible only if VMware Blast is the preferred protocol.

Prerequisites

Depending on the Horizon Agent version that is installed, a Horizon administrator can use agent-side group policy settings to enable or disable VMware Blast features, including H.264. For information, see "VMware Blast Policy Settings" in the *Configuring Remote Desktop Features in Horizon* document.

Procedure

1. Start Horizon Client.

2 Tap **Settings** at the bottom of the Horizon Client window and tap **VMware Blast**.

   If you are logged in to a server, the **VMware Blast** setting is visible only if VMware Blast is the preferred protocol.

3 To allow H.264 decoding in Horizon Client, tap and toggle the **H.264** option to on.

   When this option is selected (the default setting), Horizon Client uses H.264 decoding if the agent supports H.264 software or hardware encoding. If the agent does not support H.264 software or hardware encoding, Horizon Client uses JPG/PNG decoding. When this option is deselected, Horizon Client uses JPG/PNG decoding.

Results

Changes take effect the next time a user connects to a remote desktop or published application and selects the VMware Blast display protocol. Your changes do not affect existing VMware Blast sessions.

Configure the Horizon Client Default View

You can configure whether recently used remote desktops and published applications shortcuts, or server shortcuts, appear when you start Horizon Client.

Procedure

1 Tap **Settings** at the bottom of the Horizon Client window.

2 Tap **Default View**.

3 To select the default view, tap an option.

Option	Description
Recent	The **Recent** window appears when you start Horizon Client. The **Recent** window contains shortcuts to recently used remote desktops and published applications. This is the default setting.
Servers	The **Servers** window appears when you start Horizon Client. The **Servers** window contains shortcuts to the servers that you added to Horizon Client.

Results

The default view that you selected takes effect immediately.

Configure Horizon Client Data Sharing

If a Horizon administrator has opted to participate in the VMware Customer Experience Improvement Program (CEIP), VMware collects and receives anonymous data from client systems through Connection Server. You can configure whether to share this client data with Connection Server.

For information about configuring Horizon to join the CEIP, see the *Horizon Administration* document.

Data sharing is enabled by default in Horizon Client. You must configure the data sharing setting before you connect to a server. The setting is applied to all servers. You cannot change the Horizon Client data sharing setting after you connect to a server.

Procedure

1 Tap **Settings** at the bottom of the Horizon Client window and tap **Allow Data Sharing**.

2 Tap to toggle the **Allow Data Sharing** setting to on or off.

Horizon Client Data Collected by VMware

If a Horizon administrator has opted to participate in the customer experience improvement program, and data sharing is enabled on the client system, VMware collects data about the client system.

VMware collects data about client systems to prioritize hardware and software compatibility. If your Horizon administrator has opted to participate in the customer experience improvement program, VMware collects anonymous data about your deployment to respond better to customer requirements. VMware does not collect data that identifies your organization. Horizon Client information is sent first to the Connection Server instance and then to VMware, along with data about Connection Server, desktop pools, and remote desktops.

The information is encrypted when it is in transit to the Connection Server instance. The information on the client system is logged unencrypted in a user-specific directory. The logs do not contain personally identifiable information.

A Horizon administrator can select whether to participate in the VMware customer experience improvement program when installing Connection Server or by setting an option in Horizon Console after the installation.

Table 1-1. Data Collected from Horizon Clients for the Customer Experience Improvement Program

Description	Is This Field Made Anonymous?
Company that produced the Horizon Client application	No
Product name	No
Client product version	No
Client binary architecture	No
Client build name	No
Host operating system	No
Host operating system kernel	No
Host operating system architecture	No
Host system model	No
Host system CPU	No

Table 1-1. Data Collected from Horizon Clients for the Customer Experience Improvement Program (continued)

Description	Is This Field Made Anonymous?
Number of cores in the host system's processor	No
MB of memory on the host system	No
Number of USB devices connected	No
Maximum concurrent USB device connections	No
USB device vendor ID	No
USB device product ID	No
USB device family	No
USB device use count	No

Using URIs to Configure Horizon Client

2

You can use uniform resource identifiers (URIs) to create web page or email links that end users can click to start Horizon Client, connect to a server, or open a remote desktop or published application.

You create these links by constructing URIs that provide some or all the following information, so that your end users do not need to supply it.

- Server address
- Port number for the server
- Active Directory user name
- RADIUS or RSA SecurID user name, if different from the Active Directory user name
- Domain name
- Remote desktop or published application display name
- Actions including reset, log out, and start session

To construct a URI, you use the `vmware-view` URI scheme with Horizon Client specific path and query parts.

To use URIs to start Horizon Client, Horizon Client must already be installed on client computers.

This chapter includes the following topics:

Syntax for Creating vmware-view URIs

URI syntax includes the `vmware-view` URI scheme, a path part to specify the remote desktop or published application, and, optionally, a query to specify remote desktop or published application actions or configuration options.

URI Specification

Use the following syntax to create URIs to start Horizon Client.

```
vmware-view://[authority-part][/path-part][?query-part]
```

The only required element is the URI scheme, `vmware-view`. Because the scheme name is case-sensitive for some versions of some client operating systems, type `vmware-view`.

Important In all parts, non-ASCII characters must first be encoded according to UTF-8 [STD63], and then each octet of the corresponding UTF-8 sequence must be percent-encoded to be represented as URI characters.

For information about encoding for ASCII characters, see the URL encoding reference at http://www.utf8-chartable.de/.

authority-part

The server address and, optionally, a user name, a non-default port number, or both. Underscores (_) are not supported in server names. Server names must conform to DNS syntax.

To specify a user name, use the following syntax.

```
user1@server-address
```

You cannot specify a UPN address, which includes the domain. To specify the domain, you can use the `domainName` query part in the URI.

To specify a port number, use the following syntax.

```
server-address:port-number
```

path-part

The display name of the remote desktop or published application. The display name is specified in Horizon Console when the desktop pool or application pool is created. If the display name contains a space, use the **`%20`** encoding mechanism to represent the space.

Alternatively, you can specify a desktop or application ID, which is a path string that includes the desktop or application pool ID. To find a desktop or application ID, open ADSI Edit on the Connection Server host, navigate to `DC=vdi,dc=vmware,dc=int`, and select the `OU=Applications` node. All the desktop and application pools are listed. The `distinguishedName` attribute specifies the ID value. You must encode the ID value before you

specify it in a URI, for example, `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`.

Note More than one remote desktop or published application can have the same display name, but the desktop and application ID is unique. To specify a particular remote desktop or published application, use the desktop or application ID rather than the display name.

query-part

The configuration options to use, or the remote desktop or published application actions to perform. Queries are not case-sensitive. To use multiple queries, use an ampersand (&) between the queries. If the queries conflict, Horizon Client uses the last query in the list. Use the following syntax.

```
query1=value1[&query2=value2...]
```

Supported Queries

The following queries are supported for this type of Horizon Client. If you are creating URIs for multiple types of clients, such as desktop clients and mobile clients, see the installation and setup guide for each type of client system for the list of supported queries.

action

Table 2-1. Values That Can Be Used with the action Query

Value	Description
`browse`	Displays a list of available remote desktops and published applications hosted on the specified server. You are not required to specify a remote desktop or published application when using this action. If you use the `browse` action and specify a remote desktop or published application, the remote desktop or published application is highlighted in the list of available items.
`start-session`	Opens the specified remote desktop or published application. If no action query is provided and the remote desktop or published application name is provided, `start-session` is the default action.
`reset`	Shuts down and restarts the specified remote desktop or published application. Unsaved data is lost. Resetting a remote desktop is the same as pressing the Reset button on a physical PC.
`restart`	Shuts down and restarts the specified remote desktop. Restarting a remote desktop is the same as the Windows operating system restart command. The operating system usually prompts the user to save any unsaved data before it restarts.
`logoff`	Logs the user out of the guest operating system in the remote desktop. If you specify a published application, the action is ignored or the end user sees the warning message "Invalid URI action."

args

Specifies command-line arguments to add when the published application starts. Use the syntax `args=value`, where *value* is a string. Use percent encoding for the following characters:

- For a colon (:), use **%3A**
- For a back slash (\), use **%5C**
- For a space ( ), use **%20**
- For a double quotation mark ("), use **%22**

For example, to specify the filename "`My new file.txt`" for the Notepad++ application, use **%22My%20new%20file.txt%22**.

appProtocol

For published applications, valid values are **PCOIP** and **BLAST**. For example, to specify PCoIP, use the syntax **appProtocol=PCOIP**.

defaultLaunchView

Sets the default view for when Horizon Client starts. Valid values are **recent** and **servers**.

desktopProtocol

For remote desktops, valid values are **PCOIP** and **BLAST**. For example, to specify PCoIP, use the syntax **desktopProtocol=PCOIP**.

domainName

Specifies the NETBIOS domain name associated with the user who is connecting to the remote desktop or published application. For example, you might use `mycompany` rather than `mycompany.com`.

tokenUserName

Specifies the RSA or RADIUS user name. Use this query only if the RSA or RADIUS user name is different from the Active Directory user name. If you do not specify this query and RSA or RADIUS authentication is required, Horizon Client uses the Windows user name. The syntax is **tokenUserName=*name***.

Examples of vmware-view URIs

You can use the `vmware-view` URI scheme to create hypertext links or buttons and include these links in email or on a Web page. For example, an end user can click a URI link to start a remote desktop with the startup options that you specify.

URI Syntax Examples

Each URI example is followed by a description of what the end user sees after clicking the URI link.

1 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session`

Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, the client connects to the remote desktop that has the display name `Primary Desktop`, and the user is logged in to the guest operating system.

Note In this example, the default display protocol and window size are used. The default display protocol is PCoIP and the default window size is full screen.

2 `vmware-view://view.mycompany.com/cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`

Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, the client connects to the remote desktop that has the desktop ID `CN=win7-32,OU=Applications,DC=vdi,DC=vmware,DC=int` (encoded value `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`).

3 `vmware-view://view.mycompany.com:7555/Primary%20Desktop`

This URI has the same effect as the previous example, except that it uses the nondefault port of 7555 for the Connection Server instance. (The default port is 443.) Because a remote desktop identifier is provided, the remote desktop opens, even though the `start-session` action is not included in the URI.

4 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCOIP`

Horizon Client starts and connects to the `view.mycompany.com` server. In the login dialog box, the **User name** text box is populated with `fred`. The user must supply the domain name and password. After a successful login, the client connects to the remote desktop that has the display name `Finance Desktop`, and the user is logged in to the guest operating system. The connection uses the PCoIP display protocol.

5 `vmware-view://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST`

Horizon Client starts and connects to the `view.mycompany.com` server. In the login dialog box, the user must supply the user name, domain name, and password. After a successful login, the client connects to the published application that has the display name `Calculator`. The connection uses the VMware Blast display protocol.

6 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany`

Horizon Client starts and connects to the `view.mycompany.com` server. In the login dialog box, the **User name** text box is populated with `fred`, and the **Domain** text box is populated with `mycompany`. The user must supply only a password. After a successful login, the client connects to the remote desktop that has the display name `Finance Desktop`, and the user is logged in to the guest operating system.

7
```
vmware-view://view.mycompany.com/
```

Horizon Client starts and the user is taken to the login prompt for connecting to the `view.mycompany.com` server.

8
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=reset
```

Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, Horizon Client shows a dialog box that prompts the user to confirm the reset operation for `Primary Desktop`.

Note This action is available only if a Horizon administrator has enabled the reset feature for the remote desktop.

9
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=restart
```

Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, Horizon Client shows a dialog box that prompts the user to confirm the restart operation for `Primary Desktop`.

Note This action is available only if a Horizon administrator has enabled the restart feature for the remote desktop.

10
```
vmware-view://
```

If Horizon Client is already running, it comes to the foreground. If Horizon Client is not running, it starts.

11
```
vmware-view://?defaultlaunchview=recent
```

Horizon Client starts and the user sees the **Recent** window.

12
```
vmware-view://10.10.10.10/My%20Notepad++?args=%22My%20new%20file.txt%22
```

Starts My Notepad++ on server 10.10.10.10 and passes the argument `My new file.txt` in the published application start command. The filename is enclosed in double quotes because it contains spaces.

13
```
vmware-view://10.10.10.10/Notepad++%2012?args=a.txt%20b.txt
```

Starts Notepad++ 12 on server 10.10.10.10 and passes the argument `a.text b.txt` in the published application start command. Because the argument is not enclosed in quotes, a space separates the filenames and the two files are opened separately in Notepad++.

Note Published applications can differ in the way that they use command-line arguments. For example, if you pass the argument `a.txt b.txt` to WordPad, WordPad opens only one file, `a.txt`.

HTML Code Examples

You can use URIs to make hypertext links and buttons to include in emails or on Web pages. The following examples show how to use the URI from the first URI example to code the hypertext link labeled **Test Link** and a button labeled **TestButton**.

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Test Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>

</body>
</html>
```

Managing Remote Desktop and Published Application Connections

3

End users can use Horizon Client to connect to a server, edit the list of servers they connect to, log in to or off of remote desktops, and use published applications. For troubleshooting purposes, end users can also reset remote desktops and published applications.

Depending on how you configure policies for remote desktops, end users might be able to perform many operations on their remote desktops.

This chapter includes the following topics:

Setting the Certificate Checking Mode in Horizon Client

Server certificate checking occurs for connections between Horizon Client and a server. A certificate is a digital form of identification, similar to a passport or a driver's license.

Server certificate checking includes the following checks:

- Is the certificate intended for a purpose other than verifying the identity of the sender and encrypting server communications? That is, is it the correct type of certificate?
- Has the certificate expired, or is it valid only in the future? That is, is the certificate valid according to the computer clock?
- Does the common name on the certificate match the host name of the server that sends it? A mismatch can occur if a load balancer redirects Horizon Client to a server that has a certificate that does not match the host name entered in Horizon Client. Another reason a mismatch can occur is if you enter an IP address rather than a host name in the client.
- Is the certificate signed by an unknown or untrusted certificate authority (CA)? Self-signed certificates are one type of untrusted CA. To pass this check, the certificate's chain of trust must be rooted in the device's local certificate store.

For information about distributing a self-signed root certificate that users can install on their iOS devices, see the instructions on the Apple website. For example, for iPads, see http://www.apple.com/ipad/business/docs/iPad_Certificates.pdf.

To set the certificate checking mode, start Horizon Client, tap **Settings** at the bottom of the Horizon Client window, and tap **Certificate Verification Mode**. You can select one of the following options.

- **Never connect to untrusted servers**. This setting means that you cannot connect to the server if any of the certificate checks fail. An error message lists the checks that failed.
- **Warn before connecting to untrusted servers**. This setting means that you can click **Continue** to ignore the warning if a certificate check fails because the server uses a self-signed certificate. For self-signed certificates, the certificate name is not required to match the server name that you entered in Horizon Client. You can also receive a warning if the certificate has expired.
- **Do not verify server identity certificates**. This setting means that no certificate checking occurs.

If an administrator later installs a security certificate from a trusted certificate authority and all certificate checks pass when you connect, this trusted connection is remembered for that specific server. In the future, if that server ever presents a self-signed certificate again, the connection fails. After a particular server presents a fully verifiable certificate, it must always do so.

Connect to a Remote Desktop or Published Application

To connect to a remote desktop or published application, you must provide the name of a server and supply credentials for your user account.

Before you have end users access their remote desktops and published applications, test that you can connect to a remote desktop or published application from a client device. You might need to specify a server and supply credentials for your user account.

Prerequisites

- Obtain login credentials, such as an Active Directory user name and password, RSA SecurID user name and passcode, or RADIUS authentication credentials.
- Obtain the NETBIOS domain name for logging in. For example, you might use `mycompany` rather than `mycompany.com`.
- Perform the administrative tasks described in Preparing Connection Server for Horizon Client.
- If you are outside the corporate network and require a VPN connection to access remote desktops and published applications, verify that the client device is set up to use a VPN connection and turn on that connection.
- Verify that you have the fully qualified domain name (FQDN) of the server that provides access to the remote desktop or published application. Underscores (_) are not supported in server names. If the port is not 443, you also need the port number.
- If you plan to use embedded RSA SecurID software, verify that you have the correct CT-KIP URL and activation code. See Using Embedded RSA SecurID Software Tokens.
- Configure the certificate checking mode for the certificate presented by the server. See Setting the Certificate Checking Mode in Horizon Client.
- If you plan to use Touch ID to authenticate, add at least one fingerprint in the Touch ID & Passcode setting on the iOS device. For complete Touch ID authentication requirements, see Touch ID Authentication Requirements.
- If you plan to use Face ID authentication, verify that the Face ID option is enabled and a Face ID scan is enrolled on the client device. For complete Face ID authentication requirements, see Face ID Authentication Requirements.

Procedure

1. If a VPN connection is required, turn on the VPN.
2. Open the **Horizon** app.

3 Connect to a server.

Option	Action
Connect to a new server	Enter the name of a server, enter a description (optional), and tap **Connect**. If a server has already been added, tap **New** in the upper-right corner of the window instead.
Connect to an existing server	Tap the server shortcut in the **Servers** window.

Connections between Horizon Client and servers always use TLS. The default port for TLS connections is 443. If the server is not configured to use the default port, use the format *servername*:*port*, for example, `view.company.com:1443`.

4 If a smart card is required or optional, select the smart card certificate to use and enter your PIN.

If the smart card has only one certificate, that certificate is already selected. If there are many certificates, you can scroll through the certificates.

5 If you are prompted for RSA SecurID credentials or RADIUS authentication credentials, type your credentials, or, if you plan to use an embedded RSA SecurID token, install an embedded token.

Option	Action
Use an existing token	If you use a hardware authentication token or software authentication token on a smart phone, enter your user name and passcode. The passcode might include both a PIN and the generated number on the token.
Install a software token	a Tap **External Token**. b In the Install Software Token dialog box, paste the CT-KIP URL or CTFString URL that your system administrator sent to you in email. If the URL contains an activation code, you do not need to enter a value in the **Password or Activation Code** text box.

6 If you are prompted a second time for RSA SecurID credentials or RADIUS authentication credentials, enter the next generated number on the token.

Do not enter your PIN, and do not enter the same generated number that you entered before. If necessary, wait until a new number is generated.

If this step is required, it is required only when you mistype the first passcode or when configuration settings in the RSA server change.

7 (Optional) To use Touch ID to authenticate, tap the Touch ID (fingerprint) icon on the right-side of the **Password** text box.

When Touch ID is disabled, the icon is grey. When Touch ID is enabled, the icon turns green. Touch ID authentication is available only if biometric authentication is enabled on the server and you have not previously authenticated with Touch ID.

8 (Optional) To use Face ID to authenticate, tap the Face ID (face) icon on the right-side of the **Password** text box.

When Face ID is disabled, the icon is grey. When Face ID is enabled, the icon turns green. Face ID authentication is available only if biometric authentication is enabled on the server and you have not previously authenticated with Face ID.

9 If you are prompted for a user name and password, supply your Active Directory credentials.

a Type the user name and password of a user who is entitled to use at least one desktop or application pool.

b Select a domain.

If the **Domain** drop-down menu is hidden, type the user name as *username@domain* or *domain\username*.

c (Optional) Tap to toggle the **Remember this Password** option to on if your system administrator has enabled this feature and if the server certificate can be fully verified.

d Tap **Login**.

If Touch ID or Face ID is enabled and you are logging in for the first time, your Active Directory credentials are stored securely in the iOS device's Keychain for future use.

10 If you are prompted for Touch ID authentication, place your finger on the **Home** button.

11 If you are prompted for Face ID authentication, glance at the device.

The first time Horizon Client tries to use Face ID to authenticate, iOS prompts you to allow Horizon Client to use Face ID. If you do not want to use Face ID authentication, tap **Don't Allow** to enter a user name and password instead.

12 (Optional) To select the display protocol to use, tap **Settings** at the bottom of the Horizon Client window and tap **Preferred Protocol**.

VMware Blast provides better battery life and is the best protocol for high-end 3D and mobile device users.

13 Tap a remote desktop or published application to connect to it.

If you are connecting to a published desktop, and if the desktop is already set to use the Microsoft RDP display protocol, you cannot connect immediately. You are prompted to have the system log you off the remote operating system so that a connection can be made with the PCoIP display protocol or the VMware Blast display protocol.

Results

After you connect to a remote desktop or published application for the first time, Horizon Client saves a shortcut for the remote desktop or published application on the **Recent** window. The next time you connect to the remote desktop or published application, you can tap the shortcut instead of tapping the server shortcut.

Share Access to Local Storage with Client Drive Redirection

You can configure Horizon Client to share local storage with a remote desktop or published application. This feature is called client drive redirection.

In a Windows remote desktop or published application, local storage appears in the **Documents (Z:)** network folder. You can copy files from this network folder to a remote desktop, and you can copy files from a remote desktop to this network folder. You can also edit, delete, and rename the files and folders in this network folder from a remote desktop.

Prerequisites

- Enable the client drive redirection feature. This task involves enabling the agent **Client Drive Redirection** option. It can also include setting policies or registry settings to control client drive redirection behavior. For more information, see the *Configuring Remote Desktop Features in Horizon* document.
- Verify that iOS 11 or later is installed on the iOS device.

Procedure

1. Tap **Settings** at the bottom of the Horizon Client window to open the Settings window and tap **File Sharing**.
2. To enable client drive redirection, tap **File Sharing** in the Settings window and toggle the option to on.
3. Connect to a remote desktop or published application.

What to do next

Verify your changes in the remote desktop or published application.

- In a Windows remote desktop, open the network folder named **Documents (Z:)**.
- In a published application, select **File > Open** or **File > Save As**, if applicable and navigate to the network folder **Documents (Z:)**.

Manage Saved Servers

When you connect to a server, Horizon Client saves a shortcut for the server to the **Servers** window. Horizon Client saves a server shortcut, even if you mistype the name or type the wrong IP address. You can edit and remove server shortcuts.

Procedure

1. Tap **Servers** (cloud icon) at the bottom of the window to display the saved servers.

2 Touch and hold the server shortcut until the context menu appears.

Option	Action
Change the user name, domain, server name, or description	a Tap **Edit Server** in the context menu. b Make your changes on the **Edit Server** window. c Tap **Update** to save your changes.
Remove a server shortcut	Tap **Delete Server** in the context menu. When you remove a server shortcut, the remote desktop and published application shortcuts associated with the server are also deleted.
Forget a saved password	Tap **Forget Password** in the context menu. This option is available only if you previously saved your password.
Disable Touch ID	Tap **Sign Out**. This option is available only if you previously enabled Touch ID.
Disable Face ID	Tap **Sign Out**. This option is available only if you previously enabled Face ID.

Select a Favorite Remote Desktop or Published Application

You can select favorite remote desktops and published applications. Shortcuts for favorite items are identified by a star and appear on the **Favorites** tab. Favorite items are saved after you log off from the server.

Prerequisites

Obtain the credentials for connecting to the server, such as a user name and password or RSA SecurID and passcode.

Procedure

1 To connect to the server, tap **Servers** (cloud icon) at the bottom of the window and tap the server icon.

2 If prompted, supply your RSA user name and passcode, your Active Directory user name and password, or both.

3 To select or deselect a favorite remote desktop or published application, perform these steps.

Option	Action
Select a favorite	Touch and hold the remote desktop or published application shortcut until the context menu appears and tap **Mark as Favorite**. A star appears in the upper-right corner of the shortcut and the shortcut appears on the **Favorites** window.
Deselect a favorite	Touch and hold the remote desktop or published application shortcut until the context menu appears and tap **Unmark Favorite**. A star no longer appears in the upper-right corner of the shortcut and the shortcuts disappears from the **Favorites** window.

4 (Optional) To see only favorite remote desktops or published applications, tap **Favorites** (star icon) at the bottom of the window.

   You can tap **All** (cloud icon) at the bottom of the window to display all the available remote desktops and published applications.

Disconnecting From a Remote Desktop or Published Application

When you are logged in to a remote desktop, you can disconnect without logging off so that applications remain open in the remote desktop. You can also disconnect from a published application so that the published application remains open.

To disconnect from a remote desktop or published application, tap the Horizon Client Tools radial menu icon and tap the **Disconnect** icon. The Horizon Client Tools radial menu icon appears in the middle of the window when you are connected to a remote desktop or published application. For more information, see Using the Horizon Client Tools on a Mobile Device.

Note A Horizon administrator can configure a remote desktop to log off when it is disconnected. In that case, any open applications in the remote desktop are closed.

Log Off From a Remote Desktop

You can log off from a remote desktop, even if the remote desktop is not open in Horizon Client. If the remote desktop is open in Horizon Client, you can use the Windows **Start** menu to log off.

Prerequisites

Obtain credentials for logging in, such as an Active Directory user name and password, RSA SecurID user name and passcode, or RADIUS authentication user name and passcode.

Procedure

1 Tap **Servers** (cloud icon) at the bottom of the Horizon Client window and tap the server shortcut.

2 If prompted, supply an RSA user name and passcode, an Active Directory user name and password, or both.

3 Touch and hold the remote desktop shortcut until the context menu appears.

4 Tap **Log Off** in the context menu.

Results

The remote desktop is disconnected after you are logged off. Any unsaved files that are open on the remote desktop are closed during the log out operation.

What to do next

Disconnect from the server. See Disconnecting From a Server.

Disconnecting From a Server

After you have finished using a remote desktop or published application, you can disconnect from the server.

To disconnect from a server, tap the **Logout** button in the upper-left corner of the Horizon Client window.

Manage Remote Desktop and Published Application Shortcuts

After you connect to a remote desktop or published application, Horizon Client saves a shortcut for the item. You can rearrange and remove these shortcuts.

If you have many remote desktop and published application shortcuts, the shortcuts might appear on multiple pages. You can swipe across the pages to see more shortcuts. Horizon Client creates pages, as needed, to accommodate all your shortcuts.

Procedure

- To remove a remote desktop or published application shortcut from the **Recent** window, perform these steps.
  a. Touch and hold the shortcut.
  b. Tap the **X** button.
- To move a remote desktop or published application shortcut, touch and hold the shortcut, drag it to the new location, and tap **Done**.

  You cannot drag a shortcut to another page unless that page exists.

Using 3D Touch with Horizon Client

If you have a 3D Touch-enabled iPhone 6s or iPhone 6s Plus, you can use Peek and Pop gestures to interact with Horizon Client.

Using Peek and Pop with the Horizon app

You can Peek at the **Horizon** app on the iOS device's Home screen to show a quick action menu. In the quick action menu, you can tap **Connect to Most Recent Server** to connect to the most recently used server. If a recent server does not exist, you can tap the **Connect to Most Recent Server** item to add a new server.

After you connect to a remote desktop or published application, Horizon Client adds a shortcut to the remote desktop or published application to the quick action menu. For example, if you connect to a remote desktop named Win7, Horizon Client adds **Connect to Win7**. You can tap a shortcut to connect to a remote desktop or published application.

The **Horizon** icon quick action menu can contain up to three shortcuts.

Using Peek and Pop Inside Horizon Client

On the desktop and application selection window, you can Peek at a remote desktop or published application to show a quick action menu. You can tap items in the quick action menu to connect, log off, mark a favorite, and perform other actions, depending on the remote desktop or published application. You can also Pop into a remote desktop or published application to connect to it.

Quick action menus are also available on the **Servers**, **Recent**, and **Favorites** windows. For example, on the **Servers** window, you can Peek at a saved server and tap items in the quick action menu to edit, remove, or connect to the server. On the **Recent** window, you can Peek at a remote desktop or published application shortcut and tap items in the quick action menu to remove the shortcut or connect to the remote desktop or published application. You can also Pop into a saved server or remote desktop or published application shortcut to connect to it.

Enabling Peek for the Horizon Client Tools

By default, the Horizon Client Tools radial menu icon appears in the middle of the window when you are connected to a remote desktop or published application. You can tap the radial menu icon to expand the menu and display icons for each tool, which you tap to select. For pictures of the radial menu icon and tools icons, see Using the Horizon Client Tools on a Mobile Device.

If you enable Peek for the Horizon Client Tools, the Horizon Client Tools radial menu icon does not appear. To display the icons for each tool, press deeply on any place on the window.

To enable Peek for the Horizon Client Tools, tap **Settings** at the bottom of the Horizon Client window, tap **Touch**, and toggle the **Peek for the menu** setting to on. If you are connected to a remote desktop or published application, you can access settings by tapping the **Settings** (gear) icon in the Horizon Client Tools radial menu.

Using Spotlight Search with Horizon Client

On an iOS 9 or later device, you can use Spotlight search to search for and connect to remote desktops and published applications.

When you log in to a server in Horizon Client, the remote desktops and published applications on the server are added to the Spotlight index. Only the remote desktops and published applications on the last server to which you logged in are indexed.

To use Spotlight search to find a particular remote desktop or published application, type its name or a partial name in the Spotlight search field. For example, to find the remote desktop named Win 2012 RDS Desktop, you might type **`Win`** or **`RDS`**.

To use Spotlight search to find your favorite remote desktops and published applications, type **favorite** in the Spotlight search field. To search for any remote desktop or published application, type **vmware** or **horizon** in the Spotlight search field.

The search results can contain up to 10 items.

To connect to a remote desktop or published application, tap its name in the search results. If you are not currently connected to the server, the Horizon Client login window appears and you can log in.

Using Split View and Slide Over with Horizon Client

You can use Split View and Slide Over with Horizon Client on any iPad model that supports these features and is running iOS 9 or later.

With Split View and Slide Over, you can open Horizon Client and another app at the same time. You can run Horizon Client as the primary or secondary app.

If you rotate the device or slide the vertical divider that separates the primary and secondary apps, Horizon Client adjusts to fit the size of the window. If you are connected to a remote desktop and the **Resolution** setting is set to **Auto - Fit**, the remote desktop adjusts to fit the size of the window. For information about setting the resolution, see Changing the Display Resolution Setting.

Horizon Client does not support Picture in Picture.

Using the iPad Split Keyboard with Horizon Client

You can use the iPad onscreen keyboard in split mode with Horizon Client when you connect to a server and when you are working in a remote desktop. This feature is supported on any iPad model that supports the split keyboard feature.

To split the onscreen keyboard, tap inside a text field, touch and hold the **Keyboard** key in the lower-right corner of the onscreen keyboard, and tap **Split**. To merge a split keyboard, tap **Merge**.

When the onscreen keyboard is in split mode, the space between the two parts of the onscreen keyboard is transparent.

Note When the onscreen keyboard is in split mode, the accessory key bar is not available. To make the accessory key bar available, you must merge the keyboard.

Dragging Shortcuts and URIs

You can drag server, remote desktop, and published application shortcuts and Uniform Resource Identifiers (URIs).

This feature requires an iPad that is running iOS 11 or later.

You can drag a server shortcut from the Horizon Client **Servers** window into another app, such as Notes. The server shortcut appears as a URI in the other app, for example, `vmware-view://server-address`. You can drag a server address or URI from another app into the **Servers** window. You can also use this feature to reorder the server shortcuts on the **Servers** window.

After you connect to a server, you can drag a remote desktop or published application shortcut from the Horizon Client desktop and application selection window or the **Favorites** window into another app, such as Notes. The shortcut appears as a URI in the other app, for example, `vmware-view://server-name/item-name`. You can also drag a remote desktop or published application URI from another app into the desktop and application selection window, the **Favorites** window, or the **Recent** window.

For information about URI syntax, see Syntax for Creating vmware-view URIs.

Using the Horizon Client Widget

If you have an iOS 10 or later device, you can add the Horizon Client widget to the iOS device's Search screen.

To add the Horizon Client widget to the Search screen, click **Edit** on the Search screen, tap the green plus (**+**) button next to Horizon Client in the widget list, and click **Done**.

If you have never connected to a remote desktop or published application, the Horizon Client widget displays `No desktop/application was launched yet`. After you connect to a remote desktop or published application, a shortcut for the recently used remote desktop or published application appears in the widget. You can tap this shortcut to open the remote desktop or published application from the Search screen.

If you have a 3D Touch-enabled device, the Horizon Client widget appears in the quick action menu when you apply pressure to the **Horizon** app on the iOS device's Home screen.

Using a Microsoft Windows Desktop or Published Application

4

Horizon Client for iOS includes additional features to aid in navigation on iOS devices. Users can use external devices with remote desktops and published applications, copy text and images from iOS devices to remote desktops and published applications, and save documents in published applications.

This chapter includes the following topics:

Feature Support for iOS Clients

Certain guest operating systems and remote desktop features require specific Horizon Agent versions. Use this information when planning which features to make available to your end users.

Supported Windows Virtual Desktops

Windows virtual desktops are single-session virtual machines.

This version of Horizon Client works with Windows virtual desktops that have Horizon Agent 7.5 or later installed. Supported guest operating systems include Windows 7, Windows 8.x, and Windows 10, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019, with the following limitations:

- Windows Server 2019 virtual desktops require Horizon Agent 7.7 or later.
- Windows 7 and Windows 8.x virtual desktops are not supported with Horizon Agent 2006 and later.

Supported Published Desktops on RDS Hosts

RDS hosts are server computers that have Windows Remote Desktop Services and Horizon Agent installed. Multiple users can have published desktop sessions on an RDS host simultaneously. An RDS host can be either a physical machine or a virtual machine.

This version of Horizon Client works with RDS hosts that have Horizon Agent 7.5 or later installed. Supported guest operating systems include Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019, with the following limitations:

- Windows Server 2019 RDS hosts require Horizon Agent 7.7 or later.
- Window Server 2012 RDS hosts are not supported with Horizon Agent 2006 and later.

Requirements and Limitations for Specific Features

Some remote desktop features have specific requirements or limitations.

- The VMware Integrated Printing feature requires Horizon Agent 2006 or later.
- The VMware Integrated Printing feature is supported only with Windows 10, Windows Server 2016, and Windows Server 2019 remote desktops. Windows 7, Windows 8.x, and Windows Server 2012 R2 remote desktops cannot use this feature.

Supported Linux Desktops

For a list of supported Linux guest operating systems and information about supported features, see the *Setting Up Linux Desktops in Horizon* document.

Using the Unity Touch Sidebar with a Remote Desktop

You can quickly navigate to an application or file in a remote desktop from the Unity Touch sidebar. From this sidebar, you can open files and applications, switch between running applications, and minimize, maximize, restore, or close windows and applications in a remote desktop.

The Unity Touch feature is available only if a Horizon administrator has enabled it. If users have a floating desktop, users' favorite applications and files can be saved only if Windows roaming user profiles are configured for the remote desktop. A Horizon administrator can also create a default **Favorite Applications** list that end users see the first time the sidebar appears. For more information, see "Configuring Unity Touch" in the *Configuring Remote Desktop Features in Horizon* document.

If the Unity Touch feature is enabled, the sidebar appears on the left side of the window when you first connect to a remote desktop.

If the Unity Touch sidebar is closed, a tab appears on the left side of the window. You can swipe this tab to the right to open the sidebar. You can also slide the tab up or down.

From the Unity Touch sidebar, you can perform many actions in a remote desktop.

Table 4-1. Unity Touch Sidebar Actions for a Remote Desktop

Action	Procedure
Show the sidebar	Swipe the tab to the right. When the sidebar is open, you cannot perform actions on the remote desktop window or the Horizon Client Tools radial menu.
Hide the sidebar	Swipe the tab to the left to close the sidebar. When the sidebar is open, you cannot perform actions on the remote desktop window or the Horizon Client Tools radial menu. You can also touch the remote desktop window, including the Horizon Client Tools radial menu, to hide the sidebar.
Navigate to an application	Tap **All Programs** and navigate to the application just as you would from the Windows Start menu.
Navigate to a file	Tap **My Files** to access the `User` folder, and navigate to the file. **My Files** includes folders such as `My Pictures`, `My Documents`, and `Downloads`. **My Files** includes the folders in the user profile (`%USERPROFILE%` directory). If you relocate the `system` folder in the `%USERPROFILE%` directory, the **My Files** menu can also display content from the relocated folder, whether it is a local relocated folder or a network share folder.
Search for an application or file	■ Tap in the **Search** box and type the name of the application or file. ■ To use voice dictation, tap the microphone on the keyboard. ■ To launch an application or file, tap the name of the application or file in the search results. ■ To return to the home view of the sidebar, tap the **X** to close the **Search** box.
Open an application or file	Tap the name of the file or application in the sidebar. The application starts and the sidebar closes.
Switch between running applications or open windows	Tap the application name under **Running Applications**. If more than one file is open for one application, tap the chevron (**>**) next to the application to expand the list.

Table 4-1. Unity Touch Sidebar Actions for a Remote Desktop (continued)

Action	Procedure
Minimize a running application or window	1 Touch the application name under **Running Applications** and swipe from right to left. 2 Tap the **More** button that appears. 3 Tap **Minimize**.
Maximize a running application or window	1 Touch the application name under **Running Applications** and swipe from right to left. 2 Tap the **More** button that appears. 3 Tap **Maximize**.
Close a running application or window	Touch the application name under **Running Applications** and swipe from right to left. Tap the **Close** button that appears.
Restore a running application or window to its previous size and position	1 Touch the application name under **Running Applications** and swipe from right to left. 2 Tap the **More** button that appears. 3 Tap **Restore**.
Create a list of favorite applications or files	1 Search for the application or file, or tap **Manage** under the **Favorite Applications** or **Favorite Documents** list. If the **Manage** bar is not visible, tap the chevron (**>**) next to **Favorite Applications** or **Favorite Files**. 2 Tap the check box next to the names of your favorites in the search results or in the list of available applications or files. The favorite that you add last appears at the top of your favorites list. Your favorites are remembered across all of your mobile devices so that, for example, you have the same list whether using your smart phone or your tablet.
Remove an application or file from the favorites list	1 Search for the application or file, or tap **Manage** under the **Favorite Applications** or **Favorite Dcuments** list. If the **Manage** bar is not visible, tap the chevron (**>**) next to **Favorite Applications** or **Favorite Documents**. 2 Tap to remove the check mark next to the name of the application or file in the favorites list.
Reorder an application or file in the favorites list	1 Tap **Manage** under the **Favorite Applications** or **Favorite Documents** list. If the **Manage** bar is not visible, tap the chevron (**>**) next to **Favorite Applications** or **Favorite Documents**. 2 In the favorites list, touch and hold the handle on the left side of the application or file name and drag the favorite up or down the list.

Using the Unity Touch Sidebar with a Published Application

You can quickly navigate to a published application from the Unity Touch sidebar. From this sidebar, you can start published applications, switch between running published applications, and minimize, maximize, restore, or close published applications. You can also switch to a remote desktop.

The Unity Touch feature is available only if a Horizon administrator has enabled it.

If the Unity Touch feature is enabled, the Unity Touch sidebar appears on the left side of the window when you first connect to a published application. If the Unity Touch sidebar is closed, a tab appears on the left side of the window. You can swipe this tab to the right to reopen the sidebar. You can also slide the tab up or down.

From the Unity Touch sidebar, you can perform many actions on a published application.

Table 4-2. Unity Touch Sidebar Actions for a Published Application

Action	Procedure
Show the sidebar	Swipe the tab to the right to open the sidebar. When the sidebar is open, you cannot perform actions on the published application window.
Hide the sidebar	Swipe the tab to the left to close the sidebar. When the sidebar is open, you cannot perform actions on the published application window. You can also touch the published application window, including the Horizon Client Tools radial menu, to hide the sidebar.
Switch between running published applications	Tap the application under **Current Connection**. **Note** To avoid losing data, save your data before switching from a published application that is in multi-session mode.
Open a published application	Tap the name of the published application under **Available Applications** in the sidebar. The published application starts and the sidebar closes.
Close a running published application	1 Touch the published application name under **Current Connection** and swipe from right to left. 2 Tap the **Close** button that appears.
Minimize a running published application	1 Touch the published application name under **Current Connection** and swipe from right to left. 2 Tap the **More** button that appears. 3 Tap **Minimize**.
Maximize a running published application	1 Touch the published application name under **Current Connection** and swipe from right to left. 2 Tap the **More** button that appears. 3 Tap **Maximize**.
Restore a running published application	1 Touch the published application name under **Current Connection** and swipe from right to left. 2 Tap the **More** button that appears. 3 Tap **Restore**.
Switch to a remote desktop	Tap the remote desktop name under **Desktops**.

Using the Horizon Client Tools on a Mobile Device

On a mobile device, the Horizon Client Tools include buttons for displaying the onscreen keyboard, virtual touchpad, configuration settings, and a virtual keypad for arrow keys and function keys.

The Horizon Client Tools radial menu icon appears in the middle of the window when you are connected to a remote desktop or published application. Tap to expand the radial menu and display icons for each tool, which you can tap to select. Tap outside the tool icons to collapse the icons back into the radial menu icon.

The radial menu includes several tools.

Table 4-3. Radial Menu Icons

Icon	Description
	Horizon Client Tools radial menu
	Disconnect
	Onscreen keyboard (toggles to show or hide)
	Settings
	Navigation keys
	Virtual touchpad
	Gesture help

Onscreen Keyboard

The onscreen keyboard has more keys than the standard onscreen keyboard, for example, Control keys and function keys are available. To display the onscreen keyboard, tap the screen with three fingers at the same time or tap the **Keyboard** icon.

You can also use the feature that displays the onscreen keyboard whenever you tap a text field, such as in a note or new contact. If you then tap in an area that is not a text field, the keyboard is dismissed.

Important To use the three-finger tap, make sure the iOS accessibility feature for zooming is turned off. When the zoom accessibility feature is turned on, you zoom by double-tapping with three fingers, and tapping once with three fingers does nothing.

Even if you use an external keyboard, a one-row onscreen keyboard might still appear, which contains function keys, and the Ctrl, Alt, Win, and arrow keys. Some external keyboards do not have all these keys.

Sending a String of Characters

From the onscreen keyboard, tap the pen icon on the left side of the Ctrl key to display the local input buffer. Text that you type into this text box is not sent to an application until you tap **Send.** For example, if you open an application such as Notepad and tap the pen icon, the text that you type does not appear in the Notepad application until you tap **Send.**

Use this feature if you have a poor network connection. That is, use this feature if, when you type a character, the character does not immediately appear in the application. With this feature, you can quickly type up to 1,000 characters and then either tap **Send** or tap **Return** to have all 1,000 characters appear at once in the application.

Navigation Keys

Tap the **Ctrl/Page** icon in the Horizon Client Tools or onscreen keyboard to display the navigation keys. These keys include Page Up, Page Down, arrow keys, function keys, and other keys that you often use in Windows environments, such as Alt, Del, Shift, Ctrl, Win, and Esc. You can press and hold arrow keys for continuous key strokes. For a picture of the Ctrl/Page icon, see the table at the beginning of this topic.

Use the Shift key on this keypad when you need to use key combinations that include the Shift key, such as Ctrl+Shift. To tap a combination of these keys, such as Ctrl+Alt+Shift, first tap the onscreen Ctrl key. After the Ctrl key turns blue, tap the onscreen Alt key. After the Alt key turns blue, tap the onscreen Shift key. A single onscreen key is provided for the key combination Ctrl +Alt+Del.

Onscreen Touchpad and Full-Screen Touchpad

The virtual touchpad can be either regular-size, to resemble a touchpad on a laptop computer, or full screen, so that the entire device screen is a touchpad.

By default, when you tap the touchpad icon, you can touch anywhere on the screen to move the mouse pointer. The screen becomes a full-screen touchpad.

- Moving your finger around the touchpad creates a mouse pointer that moves around the remote desktop or published application.
- You can use the regular-size and full-screen virtual touchpad for single-clicking and double-clicking.
- The regular touchpad also contains left-click and right-click buttons.
- To simulate holding down the left-click button while dragging, double-tap with one finger and then drag.

  To enable this feature, use the Horizon Client Tools to display the Options dialog box, and click to toggle the **Touchpad Tap & Drag** option to on.
- You can tap with two fingers and then drag to scroll vertically.

You can drag the regular-size virtual touchpad to the side of the device so that you can use your thumb to operate the touchpad while you are holding the device.

You can make the virtual touchpad resemble the touchpad on a laptop, including right-click and left-click buttons. Tap to expand the Horizon Client Tools radial menu icon, tap the **Settings** (gear) icon, tap **Touch**, and toggle the **Full Screen Touchpad Mode** setting to off.

To adjust how quickly the pointer moves when you use the touchpad, tap to expand the Horizon Client Tools radial menu icon, tap the **Settings** (gear) icon, tap **Touch**, and drag the slider in the **Touchpad Sensitivity** option.

You can also set the **Full Screen Touchpad Mode** and **Touchpad Sensitivity** settings from the Horizon Client Settings window. Tap **Settings** at the bottom of the Horizon Client window and tap **Touch** to display the touchpad settings.

If you are logged in to a remote desktop or published application when you change the touchpad settings, your touchpad settings are retained the next time you connect to the remote desktop or published application from the same iOS device.

Gestures

VMware has created user interaction aids to help you navigate conventional Windows user interface elements on a non-Windows device.

Clicking

As in other applications, you tap to click a user interface element.

In a remote desktop, if you tap and hold for a second, a magnifying glass appears, along with a mouse pointer, for precise placement. This feature is especially helpful when you want to resize a window.

Note If the remote desktop is configured for a left-handed user, see Configure Horizon Client to Support Reversed Mouse Buttons.

Right-Clicking

The following options are available for right-clicking:

- Use the Horizon Client Tools to display the regular virtual touchpad and use the touchpad's right-click button.
- On a touch screen, tap with two fingers at nearly the same time. The right-click occurs where the first finger tapped.

Scrolling and Scrollbars

The following options are available for vertical scrolling.

- On a touch screen, tap with one or two fingers and then drag to scroll. The text under your fingers moves in the same direction as your fingers.

  Important Scrolling with one finger does not work if you have zoomed in, or when the onscreen keyboard is displayed, or when you are using the full-screen touchpad.

- Use the Horizon Client Tools to display the touchpad, tap the touchpad with two fingers, and then drag to scroll.
- Use the onscreen touchpad to move the mouse pointer and click scroll bars.

Zooming In and Out

As in other applications, pinch your fingers together or apart to zoom on a touch screen.

Window Resizing

If you use the full screen touchpad to resize a window, touch and hold one finger at the corner or side of the window and drag to resize, or double-tap with one finger and then drag.

If you use the regular-size virtual touchpad, to simulate holding down the left-click button while dragging the corner or side of a window, double-tap with one finger and then drag.

If you are not using either type of virtual touchpad, tap and hold until the magnifying glass appears at the corner or side of the window. Move your finger around until the resizing arrows appear. Lift your finger off the screen. The magnifying glass is replaced by a resizing circle. Tap this resizing circle and drag it to resize the window.

Sound, Music, and Video

If sound is turned on for your device, you can play audio in a remote desktop.

Using Native Operating System Gestures with Touch Redirection

With the touch redirection feature, you can use native operating system gestures from a touch-based mobile device in a remote desktop or published application. For example, you can touch, hold, and release an item on a Windows 8.1 remote desktop to display the item's context menu.

When touch redirection is enabled, Horizon Client local gestures, such as double-click and pinch, no longer work. You must drag the Unity Touch tab button to display the Unity Touch sidebar.

Touch redirection is enabled by default when you connect to most remote desktops.

To disable touch redirection, tap **Settings** at the bottom of the Horizon Client window, tap **Touch**, and toggle the **Windows Native Touch Gestures** setting to off. If you are connected to a remote desktop or published application, tap the **Settings** (gear) icon in the Horizon Client Tools radial menu.

Screen Resolutions and Using External Displays

You can use Horizon Client with external displays and you can change screen resolutions.

When you connect a client device to an external display or projector, Horizon Client supports certain maximum display resolutions. You can change the screen resolution that the client device uses to allow scrolling a larger screen resolution.

Enlarging the Screen Resolution for a Remote Desktop

By default, the display resolution is set so that the entire remote desktop fits inside the client device, and the remote desktop icons and task bar icons are a certain size. If you use a larger resolution, the remote desktop still fits inside the client device, but the remote desktop and taskbar icons become smaller.

You can pinch your fingers apart to zoom in and make the remote desktop larger than the device screen. You can then tap and drag to access the edges of the remote desktop.

Changing the Display Resolution Setting

To change the resolution from a remote desktop or published application, tap to expand the Horizon Client Tools radial menu icon, tap the **Settings** (gear) icon, and tap **Resolution**. You can also change the resolution from the Horizon Client Settings window. Tap **Settings** at the bottom of the Horizon Client window and tap **Resolution**.

Note Certain options, including 3/4 Scaling and No Scaling, are not available on iPhone 6 when the device is in zoomed mode. To display these options, you must exit zoomed mode.

Using High Resolution Mode

You can use the High Resolution Mode feature to obtain the best display quality in remote desktops and published applications.

To enable High Resolution Mode from the Horizon Client Settings window, tap **Settings** at the bottom of the Horizon Client window, tap **Resolution**, and tap to toggle the **High Resolution Mode** setting to on. To enable High Resolution Mode from a remote desktop or published application, tap to expand the Horizon Client Tools radial menu icon, tap the **Settings** (gear) icon, tap **Resolution**, and tap to toggle the **High Resolution Mode** setting to on.

The High Resolution Mode feature has the following requirements and limitations.

- You cannot use the High Resolution Mode feature for existing sessions. You must log out and log in to a new session for the feature to take effect.

- You must have an iPad Pro, or an iPad or iPad mini with Retina display, to use the High Resolution Mode feature.
- The High Resolution Mode feature can consume significant bandwidth. To optimize for bandwidth, set the **High Resolution Mode** setting to off.

High Resolution Mode is enabled by default.

Using External Monitors and Projectors

You can use the **Resolution** setting to set a larger resolution for external monitors and projectors.

To display the keyboard and an expanded onscreen touchpad on the device while displaying the remote desktop on the projector or attached monitor, enable the **Presentation Mode** setting. The expanded touchpad and keyboard appear when you plug the device into the external monitor. The device detects the maximum resolution provided by the external display.

You can mirror the entire device display on a projector or attached monitor, including the Unity Touch sidebar, by turning off the **Presentation Mode** setting. If you are connected to a remote desktop and the **Presentation Mode** setting is enabled, you can click **Done** to switch to mirror mode.

You can use the **Keep the screen alive during Presentation** setting to keep the display from turning off after a period of inactivity while in presentation mode.

You can configure these settings from a remote desktop or published application by tapping to expand the Horizon Client Tools radial menu icon and tapping the **Settings** (gear) icon. You can also configure these settings by tapping the **Settings** (gear) icon at the bottom of the Horizon Client window.

Hiding Sensitive Information on External Displays

When you use Horizon Client with an external monitor or projector, sensitive information, such as passwords and passcodes, is hidden to protect user data security.

Using DPI Synchronization

The DPI Synchronization feature ensures that the DPI setting in a remote desktop or published application matches the client system's DPI setting.

If DPI synchronization is disabled, display scaling is used. The Display Scaling feature scales the remote desktop or published application appropriately.

The **DPI Synchronization** agent group policy setting determines whether the DPI Synchronization feature is enabled. The feature is enabled by default. With DPI Synchronization, the DPI value in the remote session changes to match the DPI value of the client machine when you connect to a remote desktop or published application.

If the **DPI Synchronization Per Connection** agent group policy setting is enabled in addition to the **DPI Synchronization** group policy setting, DPI Synchronization is supported when you reconnect to a remote desktop. This feature is disabled by default.

For more information about the **DPI Synchronization** and **DPI Synchronization Per Connection** group policy settings, see the *Configuring Remote Desktop Features in Horizon* document.

For virtual desktops, the DPI Synchronization feature is supported on the following guest operating systems:

- 32-bit or 64-bit Windows 10
- Windows Server 2012 R2 configured as a desktop
- Windows Server 2016 configured as a desktop
- Windows Server 2019 configured as a desktop

For published desktops and published applications, the DPI Synchronization feature is supported on the following RDS hosts:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

For virtual desktops, the DPI Synchronization Per Connection feature is supported on the following guest operating systems:

- Windows 10 version 1607 and later
- Windows Server 2016 and later configured as a desktop

The DPI Synchronization Per Connection feature is not supported for published desktops or published applications.

Following are tips for using the DPI Synchronization feature.

- If you change the DPI setting on the client system, but the DPI setting does not change in the remote desktop, you might need to log out and log in again to make Horizon Client aware of the new DPI setting on the client system.
- If you start a remote session on a client system that has a DPI setting of more than 100 percent, and then use the same session on another client system that has a different DPI setting of more than 100 percent, you might need to log out and log back in to the remote session on the second client system to make DPI synchronization work on the second client system.

External Keyboards and Input Devices

You can use the iPad Keyboard Dock and Apple Wireless Keyboard (Bluetooth) external keyboards with remote desktops and published applications. On an iPad Pro, you can use the Apple Pencil as a pointer device, and you can use the Swiftpoint GT mouse on any iOS device that supports the Swiftpoint GT mouse.

Using an External Keyboard

Horizon Client automatically detects the iPad Keyboard Dock external keyboard.

To use the Apple Wireless Keyboard (Bluetooth) with a remote desktop or published application, you must first pair the keyboard with the iPad. To make the iPad detect the wireless keyboard, tap the screen with three fingers at the same time, or tap the **Keyboard** button in the Horizon Client Tools. Do not use the onscreen keyboard in split keyboard mode when you attempt to make the iPad detect the Apple Wireless Keyboard (Bluetooth) keyboard.

After the iPad detects the Apple Wireless Keyboard (Bluetooth), you cannot use the Horizon Client Tools or three-finger tap to display the onscreen keyboard. To use these features, deactivate the external keyboard by pressing its Eject key.

Note The Apple Wireless Keyboard (Bluetooth) does not input the Japanese full-width tilde correctly in remote desktops.

Using the Swiftpoint GT Mouse

To use the Swiftpoint GT Mouse with Horizon Client, see Enable a Swiftpoint GT Mouse in Horizon Client.

Note Natively connected Bluetooth and USB mice generate only touch events. Because these types of mice do not generate normal mouse events, they cannot be directly interpreted and used in remote desktops and published applications.

Using International Keyboards

You can input characters for English, Japanese, French, German, Simplified Chinese, Traditional Chinese, Korean, and Spanish.

For a remote desktop that uses a Korean or Japanese input method editor (IME), you must use an English keyboard on the iOS device. If you use a Korean or Japanese keyboard, the remote desktop Windows IME English/Korean or English/Japanese mode is not synchronized with the iOS keyboard locale.

Enable a Swiftpoint GT Mouse in Horizon Client

If you have a Swiftpoint GT mouse, you can enable it to work with remote desktops and published applications in Horizon Client.

Prerequisites

- Turn on the Swiftpoint GT mouse.
- Turn on Bluetooth on the client device.

Procedure

1. Tap **Settings** at the bottom of the Horizon Client window.

2 Tap **Mouse** on the Settings window.

3 Tap **Swiftpoint GT Mouse** and toggle the option to on.

Horizon Client shows the Swiftpoint GT mouse and an option to connect to it. If Bluetooth is not turned on, Horizon Client prompts you to go to the iOS settings and turn on Bluetooth before you pair the mouse with the client device.

4 (Optional) To learn more about using the Swiftpoint GT mouse with Horizon Client, click the http://www.swiftpoint.com/vmware link.

Results

After you pair the mouse with the device, mouse actions are redirected to remote desktops and published applications that you open with Horizon Client

Using the Real-Time Audio-Video Feature

With the Real-Time Audio-Video feature, you can use the client device's built-in cameras and microphones in a remote desktop or published application. Real-Time Audio-Video is compatible with standard audio devices and with standard conferencing applications such as Skype, WebEx, and Google Hangouts.

Real-Time Audio-Video is enabled by default when you install Horizon Client on the client device.

For information about setting up the Real-Time Audio-Video feature for remote desktops and published applications, see the *Configuring Remote Desktop Features in Horizon* document.

The first time you use a camera or microphone, Horizon Client prompts you for permission to access it. You must grant permission for the microphone or camera to work with the remote desktop or published application. You can enable and disable access to the microphone by changing the Microphone privacy setting for Horizon Client in the iOS Settings app. You can enable and disable access to the camera by changing the Camera privacy setting for Horizon Client in the iOS Settings app. If you deny access to both the microphone and the camera, Horizon Client disables the Real-Time Audio-Video feature.

Horizon Client gives up control of the microphone and camera when Horizon Client is in the background, for example, when you switch to another app.

Note Because Horizon Client does not adjust the remote desktop orientation in Presentation mode when you rotate the client device, the Real-Time Audio Video feature does not adjust the camera direction when you rotate the client device.

If the client device has both a front and a back camera, you can select the camera to use in the remote desktop or published application. You can also select the video resolution to use. For information about configuring these camera settings in Horizon Client, see Configure Camera Settings for the Real-Time Audio-Video Feature.

Configure Camera Settings for the Real-Time Audio-Video Feature

With the Real-Time Audio-Video feature, you can use the client device's built-in cameras in a remote desktop or published application. If the client device has both a front and a back camera, you can select the camera to use in the remote desktop or published application. You can also select the video resolution to use.

Prerequisites

To change the video resolution, you must not be connected to a remote desktop or published application.

Procedure

1. In Horizon Client, open **Settings** and tap **Camera**.
   - If you are not connected to a remote desktop or published application, tap **Settings** at the bottom of the Horizon Client window.
   - If you are connected to a remote desktop or published application, tap the **Settings** (gear) icon in the Horizon Client Tools radial menu.
2. To select the camera to use with the Real-Time Audio-Video feature, tap **Front** or **Rear**.
3. To set the video resolution, select one of the video resolution settings.

   You cannot change the video resolution if you are connected to a remote desktop or published application.

   If you select the **Default** setting, the video resolution is based on the **Resolution - Default image resolution width in pixels** and **Resolution - Default image resolution height in pixels** agent group policy settings for the remote desktop. For more information, see "Real-Time Audio-Video Group Policy Settings" in the *Configuring Remote Desktop Features in Horizon* document. If you select **High**, **Medium**, or **Low**, the video resolution on the remote desktop is overridden.

Configure Horizon Client to Support Reversed Mouse Buttons

If the primary and secondary mouse buttons are switched in a remote desktop, you can configure Horizon Client to support reversed mouse buttons.

If you set the mouse properties inside the remote desktop so that the primary mouse button is on the right side, as many left-handed people do, you must turn on the **Left Handed Mode** option in Horizon Client. If you do not turn on this option when the mouse buttons are reversed, a single tap acts as a click of the secondary mouse button. For example, a single tap might display a context menu rather than selecting text or inserting a cursor.

Procedure

- If you are already connected to the remote desktop, perform these steps.
  a Tap to expand the Horizon Client Tools radial menu icon and tap the **Settings** (gear) icon to open the Settings window.
  b Tap **Touch** on the Settings window.
  c Tap **Left Handed Mode** to toggle the option to on.
  d Tap **Done** to close the Settings window.
- If you are not connected to the remote desktop, perform these steps.
  a Tap **Settings** at the bottom of the Horizon Client window.
  b Tap **Touch** on the Settings window.
  c Tap **Left Handed Mode** to toggle the option to on.

Results

A single tap now acts as a click with the primary mouse button.

Copying and Pasting Text and Images

By default, you can copy and paste from the iOS device to a remote desktop or published application. You can also copy and paste from a remote desktop or published application to the iOS device, or between two remote desktops or published applications, if a Horizon administrator enables these features. Supported file formats include plain text, images, and Rich Text Format (RTF).

Data that you copy to the clipboard on the iOS device is copied to the clipboard on the remote desktop when you log in to the remote desktop. If you are logged in to a remote desktop, data that you copy to the clipboard on the remote desktop is copied to the clipboard on the iOS device.

The copy and paste feature has the following limitations.

- If RTF data contains images, the images are lost when Horizon Client synchronizes the RTF data in the clipboard on the remote desktop with the data in the clipboard on the iOS device.
- If the text and RTF data together use less than maximum clipboard size, the formatted text is pasted. Often RTF data cannot be truncated. If the text and formatting use more than the maximum clipboard size amount, the RTF data is discarded, and plain text is pasted. If you are unable to paste all the formatted text you selected in one operation, you might need to copy and paste smaller amounts in each operation.
- You might not be able to copy and paste a certain image, even though it does not exceed the clipboard size. This problem occurs when Horizon Client converts the image to PNG format and the PNG image exceeds the clipboard size. Horizon Client converts all images to PNG format during the copy and paste operation.

A Horizon administrator can configure this feature so that copy and paste operations are allowed only from the iOS device to a remote desktop or published application, or only from a remote desktop or published application to the iOS device, or both, or neither.

A Horizon administrator can configure the copy and paste behavior by setting group policies that pertain to Horizon Agent, including changing the clipboard size. The default clipboard size is 1 MB. The clipboard can accommodate up to 16 MB of data. Depending on the Horizon server and agent version, a Horizon administrator might also use group policies to restrict clipboard formats during copy and paste operations, or use Smart Policies. For information, see the *Configuring Remote Desktop Features in Horizon* document.

Logging Copy and Paste Activity

When you enable the clipboard audit feature, Horizon Agent records information about copy and paste activity in an event log on the agent machine. The clipboard audit feature is disabled by default.

To enable the clipboard audit feature, you must configure the **Configure clipboard audit** group policy setting for VMware Blast or PCoIP.

You can optionally configure the **Whether block clipboard redirection to client side when client doesn't support audit** group policy setting for VMware Blast or PCoIP to specify whether to block clipboard redirection to clients that do not support the clipboard audit feature.

For information about configuring these group policy settings, see the "VMware Blast Policy Settings" and "PCoIP Clipboard Settings" topics in the *Configuring Remote Desktop Features in Horizon* document.

This feature requires Horizon Agent 7.7 or later on the agent machine.

The event log where information about copy and paste activity is recorded is named VMware Horizon RX Audit. To view the event log on the agent machine, use the Windows event viewer. To view the event log from a centralized location, configure VMware Log Insight or Windows Event Collector. For information about Log Insight, go to https://docs.vmware.com/en/vRealize-Log-Insight/index.html. For information about Windows Event Collector, see the Microsoft documentation.

Dragging Text and Images

If you have an iPad that is running iOS 11 or later, you can drag text and images from the client device to a published application or an open application in a remote desktop. For example, you can drag text from Safari on the iPad and drop it into the WordPad application in a remote desktop. Both plain text and Rich Text Format (RTF) text are supported.

Horizon administrators can configure drag and drop behavior by setting group policies that pertain to Horizon Agent, including changing the clipboard size. The default clipboard size is 1 MB. The clipboard can accommodate up to 16 MB of data. Depending on the Horizon server and agent version, administrators might also use group policies to restrict clipboard formats during drag and drop operations, or use Smart Policies. For information, see the *Configuring Remote Desktop Features in Horizon* document.

This feature has the following limitations.

- You cannot drag multiple images at the same time.
- You cannot drag text and images at the same time.
- You might not be able to drag a certain image, even though it does not exceed the clipboard size. This problem occurs when Horizon Client converts the image to PNG format and the PNG image exceeds the clipboard size. Horizon Client converts all images to PNG format during the drag and drop operation.
- You cannot drag text and images from a remote desktop or published application to the client device.

Printing From a Remote Desktop or Published Application

With the VMware Integrated Printing feature, you can print to an AirPrint-enabled printer from a remote desktop or published application.

To use this feature, Horizon Agent must be installed on the virtual machine or RDS host with the VMware Integrated Printing option enabled. For more information, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.

Printing from a remote desktop or published application is a two-step procedure. For example, first you select **File > Print** in a Windows application, select the virtual printer that belongs to the mobile device, and tap **Print**. Next, the device's print dialog box appears. From the device's print dialog box, you click **Print** again. You can optionally select local print options, such as number of copies, paper size, and so on.

A Horizon administrator can disable the VMware Integrated Printing feature by using the **Disable printer redirection for non-desktop client** group policy setting. For more information, see the *Configuring Remote Desktop Features in Horizon* document.

Saving Documents in a Published Application

With certain published applications, such as Microsoft Word or WordPad, you can create and save documents. Where these documents are saved depends on your company's network environment. For example, your documents might be saved to a home share mounted on your local computer.

A Horizon administrator can use the RDS Profiles group policy setting called **Set Remote Desktop Services User Home Directory** to specify where documents are saved. For more information, see the *Configuring Remote Desktop Features in Horizon* document.

Use Multiple Sessions of a Published Application From Different Client Devices

When multi-session mode is enabled for a published application, you can use multiple sessions of the same published application when you log on to the server from different client devices.

For example, if you open a published application in multi-session mode on client A, and then open the same published application on client B, the published application remains open on client A and a new session of the published application opens on client B. By comparison, when multi-session mode is disabled (single-session mode), the published application session on client A disconnects and reconnects on client B.

The multi-session mode feature has the following limitations.

- Multi-session mode does not work for applications that do not support multiple instances, such as Skype for Business.
- If the application session is disconnected while you are using a published application in multi-session mode, you are logged off automatically and any unsaved data is lost.

Prerequisites

A Horizon administrator must enable multi-session mode for the application pool. Users cannot modify the multi-session mode for a published application unless a Horizon administrator allows it. See *Setting Up Published Desktops and Applications in Horizon*. This feature requires Horizon 7 version 7.7 or later.

Procedure

1. Connect to a server.
2. Tap **Settings** at the bottom of the Horizon Client window and tap **Multi-Launch**.

   If no published applications are available to use in multi-session mode, the **Multi-Launch** setting does not appear.
3. To use a published application in multi-session mode, tap the toggle next to the published application's name to on.

   If a Horizon administrator has enforced multi-session mode for a published application, you cannot change this setting.

Multitasking

You can switch between Horizon Client and other apps without losing a remote desktop or published application connection.

Horizon Client suspends data transmission when you switch to another app. Data transmission resumes when you switch back to Horizon Client.

By default Horizon Client runs in the background for up to three minutes on iOS 9.0 and later devices. After three minutes, you can resume Horizon Client and continue using the previous remote desktop or published application session without having to reenter your credentials. You must reenter your credentials only if the server's session timeout, or idle session timeout, limit is exceeded.

Suppress the Cellular Data Warning Message

When Horizon Client detects that you are using a cellular data connection, the Network Usage dialog box appears to notify you that your remote desktop or published application connection might use a substantial portion of your data plan.

The Network Usage dialog box appears after you connect to a server and try to start a remote desktop or published application, after you tap a recent remote desktop or published application shortcut, and after you connect to a published application and try to start another published application or remote desktop from the Unity Touch sidebar. The Network Usage dialog box appears only when you start Horizon Client.

You can suppress the Network Usage dialog box after it appears. You can also set an option that always suppresses the Network Usage dialog box.

Procedure

- To suppress the Network Usage dialog box after it appears in Horizon Client, tap **Never Remind** in the Network Usage dialog box.
- To set an option to always suppress the Network Usage dialog box, tap **Settings** at the bottom of the Horizon Client window and toggle the **Cellular Data Warning** option to off.

PCoIP Client-Side Image Cache

PCoIP client-side image caching stores image content on the client to avoid retransmitting data. This feature reduces bandwidth use.

The PCoIP image cache captures spatial and temporal redundancy. For example, when you scroll through a PDF document, new content appears from the bottom of the window and the oldest content disappears from the top of the window. The remaining content is constant and moves upward. The PCoIP image cache can detect this spatial and temporal redundancy.

During scrolling, because the display information sent to the client is primarily a sequence of cache indexes, using the image cache saves a significant amount of bandwidth. This efficient scrolling has benefits both on the LAN and over the WAN.

- On the LAN, where the bandwidth is relatively unconstrained, using client-side image caching delivers significant bandwidth savings.

- Over the WAN, to stay within the available bandwidth constraints, scrolling performance is degraded without client-side caching. Over the WAN, client-side caching saves bandwidth and ensures a smooth, highly responsive scrolling experience.

With client-side caching, the client stores portions of the display that were previously transmitted. The cache size is one-half the available RAM. If that amount of RAM is less than 50 MB, the cache size is 50 MB.

Troubleshooting

5

You can solve most Horizon Client problems by restarting or resetting remote desktops or published applications, or by reinstalling Horizon Client.

You can also enable log collection and send log files to VMware for troubleshooting.

This chapter includes the following topics:

Restart a Remote Desktop

If the remote desktop operating system stops responding, you might need to restart a remote desktop. Restarting a remote desktop is similar to using the Windows operating system restart command. The remote desktop operating system usually prompts you to save any unsaved data before it restarts.

You can restart a remote desktop only if a Horizon administrator has enabled the restart feature for the remote desktop.

For information about enabling the desktop restart feature, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.

Procedure

1. To connect to the server, tap **Servers** (cloud icon) at the bottom of the window and tap the server icon.
2. If prompted, supply your RSA user name and passcode, your Active Directory user name and password, or both.

3 Touch and hold the remote desktop shortcut until the context menu appears.

4 Tap **Restart** in the context menu.

Results

The operating system in the remote desktop restarts and the client disconnects and logs off from the remote desktop.

What to do next

Wait an appropriate amount of time for the system to restart before you attempt to reconnect to the remote desktop.

If restarting the remote desktop does not solve the problem, you might need to reset the remote desktop. See Reset a Remote Desktop or Published Applications.

Reset a Remote Desktop or Published Applications

You might need to reset a remote desktop if the desktop operating system stops responding and restarting the remote desktop does not solve the problem. Resetting published applications quits all open published applications.

Resetting a remote desktop is similar to pressing the Reset button on a physical PC to force the PC to restart. Any files that are open on the remote desktop are closed and are not saved.

Resetting published applications quits the applications without saving any unsaved data. All open published applications are closed, including applications that come from different RDS server farms.

You can reset a remote desktop only if a Horizon administrator has enabled the reset feature for the remote desktop.

For information about enabling the remote desktop reset feature, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.

Prerequisites

Obtain login credentials, such as an Active Directory user name and password, RSA SecurID user name and password, or RADIUS authentication user name and password.

Procedure

1 Tap **Servers** (cloud icon) at the bottom of the window and tap the server icon to connect to the server.

2 If prompted, supply your RSA user name and passcode, your Active Directory user name and password, or both.

3 Touch and hold the remote desktop or published application shortcut until the context menu appears.

4 Tap **Reset** in the context menu.

Results

When you reset a remote desktop, the operating system in the remote desktop reboots and Horizon Client disconnects and logs off from the remote desktop. When you reset a published application, all published applications quit.

What to do next

Wait an appropriate amount of time for system startup before attempting to reconnect to the remote desktop or published application.

Collecting and Sending Logging Information to VMware

You can configure Horizon Client to collect log information and send log files to VMware for troubleshooting.

If Horizon Client quits unexpectedly while log collection is enabled, it prompts you to send log files to VMware when you restart Horizon Client.

If you send log files to VMware, Horizon Client sends a message from the email account configured on the client device and attaches a GZ file that contains the last five log files. The file name contains a time stamp, for example, `Horizon_View_Client_logs_`*`timestamp`*`.log.gz`.

You can also manually retrieve and send log files at any time.

Enable Horizon Client Log Collection

When you enable log collection, Horizon Client creates log files that contain information that can help VMware troubleshoot problems with Horizon Client.

Because log collection affects the performance of Horizon Client, enable log collection only if you are experiencing a problem.

Prerequisites

Verify that an email account is configured on the device. Horizon Client uses this email account to send log files.

Procedure

1. If you are already connected to a remote desktop or published application, perform these steps:
   a. Tap to expand the Horizon Client Tools radial menu icon and tap the **Settings** (gear) icon to open the Settings window.
   b. Tap **Log Collection** on the Settings window.
   c. Tap to toggle the **Logging** option to on.
   d. Tap **Done** to close the Settings window.

2 If you are not connected to a remote desktop or published application, perform these steps:

   a Tap **Settings** at the bottom of the Horizon Client window to open the Settings window.

   b Tap **Log Collection** on the Settings window.

   c Tap to toggle the **Logging** option to on.

Results

After log collection is enabled, Horizon Client generates several log files. When Horizon Client quits unexpectedly or is exited and restarted, the log files are merged and compressed into a single GZ file. If you choose to send the log, Horizon Client attaches the GZ file to an email message.

If you switch from a running remote desktop to settings, enable log collection, and switch back to the remote desktop, you must reconnect to the remote desktop to collect a complete log file.

Manually Retrieve and Send Horizon Client Log Files

When Horizon Client log collection is enabled on the client device, you can manually retrieve and send log files at any time.

This procedure explains how to retrieve and send log files through Horizon Client. If the client device is connected to a PC or Mac, you can also use iTunes to retrieve log files.

Prerequisites

- Verify that an email account is configured on the client device. Horizon Client sends log files from this email account.
- Enable Horizon Client log collection. See Enable Horizon Client Log Collection.

Procedure

1 In Horizon Client, tap the email icon at the top of the window.

2 Type the address of the email recipient in the **To:** line and click **Send** to send the message.

   The email account configured on the client device appears in the **From:** line.

   The existing GZ log file is attached to the message. Horizon Client saves a maximum of five GZ log files. It deletes the oldest files when the GZ log file count is greater then five.

Disable Horizon Client Log Collection

Because log collection affects the performance of Horizon Client, disable log collection if you are not troubleshooting a problem.

Procedure

1 If you are already connected to a remote desktop or published application, perform these steps.
   a Tap to expand the Horizon Client Tools radial menu icon and tap the **Settings** (gear) icon to open the Settings window.
   b Tap **Log Collection** on the Settings window.
   c Tap to toggle the **Logging** option to off.
   d Tap **Done** to close the Settings window.
2 If you are not connected to a remote desktop or published application, perform these steps.
   a Tap **Settings** at the bottom of the Horizon Client window to open the Settings window.
   b Tap **Log Collection** on the Settings window.
   c Tap to toggle the **Logging** option to off.

Report Horizon Client Crash Data to VMware

You can configure Horizon Client to report crash data to VMware.

Procedure

1 Tap **Settings** at the bottom of the Horizon Client window.
2 Tap **Crash Reporting**.
3 Tap to toggle the **Crash Reporting** option to on or off.

   The setting is enabled by default.

Results

If Horizon Client stops responding, a crash log file is uploaded to the server the next time Horizon Client starts.

Horizon Client Stops Responding or the Remote Desktop Freezes

Horizon Client stops responding or a remote desktop freezes.

Problem

Horizon Client does not work or repeatedly exits unexpectedly, or the remote desktop freezes.

Cause

If the server is configured properly and the correct firewall ports are open, the cause of the problem usually relates to Horizon Client on the device or to the remote desktop operating system.

Solution

- If the remote desktop operating system freezes, use Horizon Client on the client device to reset the desktop.

  This option is available only if a Horizon administrator has enabled the desktop reset feature.
- Uninstall and reinstall the Horizon Client app on the client device.
- If resetting the remote desktop and reinstalling Horizon Client do not help, you can reset the client device, as described in the client device user guide from Apple.
- If you receive a connection error when you attempt to connect to the server, you might need to change your proxy settings.

Problem Establishing a Connection When Using a Proxy

When you attempt to connect to a server by using a proxy while on the LAN, an error sometimes occurs.

Problem

If your Horizon environment is set up to use a secure connection from a remote desktop to a server, and if the client device is configured to use an HTTP proxy, you might not connect.

Cause

Unlike Windows Internet Explorer, the client device does not have an Internet option to bypass the proxy for local addresses. When an HTTP proxy is used for browsing external addresses, and you try to connect to a server by using an internal address, you might see the error message `Could not establish connection`.

Solution

- Remove the proxy settings so that the client device no longer uses a proxy.

Connecting to a Server in Workspace ONE Mode

You cannot connect to a server directly through Horizon Client, or your remote desktop and published application entitlements are not visible in Horizon Client.

Problem

- When you try to connect to the server directly through Horizon Client, Horizon Client redirects you to the Workspace ONE portal.
- When you open a remote desktop or published application through a URI or shortcut, or when you open a local file through file association, the request redirects you to the Workspace ONE portal for authentication.

- After you open a remote desktop or published application through Workspace ONE and Horizon Client starts, you cannot see or open other entitled remote desktops or published applications in Horizon Client.

Cause

A Horizon administrator can enable Workspace ONE mode on a Connection Server instance. This behavior is normal when Workspace ONE mode is enabled on a Connection Server instance.

Solution

Use Workspace ONE to connect to a Workspace ONE enabled server and access your remote desktops and published applications.